WatchGuard® Firebox® SOHO 6 User Guide

SOHO 6.0

Using this Guide

To use this guide you need to be familiar with your computer's operating system. If you have questions about navigating in your computer's environment, please refer to your system user manual.

The following conventions are used in this guide.

Convention	Indication
Bold type	Menu commands, dialog box options, Web page options, Web page names. For example: "On the System Information page, select Disabled."
NOTE	Important information, a helpful tip or additional instructions.

Certifications and Notices

FCC Certification

This appliance has been tested and found to comply with limits for a Class A digital appliance, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This appliance may not cause harmful interference.
- This appliance must accept any interference received, including interference that may cause undesired operation.

CE Notice

The CE symbol on your WatchGuard Technologies equipment indicates that it is in compliance with the Electromagnetic Compatibility (EMC) directive and the Low Voltage Directive (LVD) of the European Union (EU).

Industry Canada

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglement sur le materiel broulleur du Canada.

VCCI Notice Class A ITE

この装置は、情報処理装置等電波障害自主規制協議会（VCCI)の基準に基づくクラス A 情報技術装置です。この装置を家庭用環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Declaration of Conformity

DECLARATION OF CONFORMITY

WatchGuard Technologies, Inc.
505 Fifth Ave. S., Suite 500
Seattle, WA 98104-3892
USA

WatchGuard Technologies Inc. hereby declares that the product(s) listed below conform to the European Union directives and standards identified in this declaration.

Product (s):

Internet Firewall, Model B0F4S16E6

EU Directive(s):

Low Voltage (73/23/EEC)
Electromagnetic Compatibility (89/336/EEC)

Standard(s):

This product has no safety requirements per the LVD
EN50022 (1998), Class A Emissions for ITE
EN50024 (1998) Immunity for ITE

Signature
Full Name Jim Cady
Position President, COO
Date 25 July 2002

WATCHGUARD SOHO SOFTWARE
END-USER LICENSE AGREEMENT

WATCHGUARD SOHO SOFTWARE
END-USER LICENSE AGREEMENT

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE
This WatchGuard SOHO Software End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD SOHO software product, which includes computer software (whether installed separately on a computer workstation or on the WatchGuard hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity service (or its equivalent) (the "SOFTWARE PRODUCT"). WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this EULA. Please read this EULA carefully.
By installing or using the SOFTWARE PRODUCT you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, WATCHGUARD will not license the SOFTWARE PRODUCT to you, and you will not have any rights in the SOFTWARE PRODUCT. In that case, promptly return the SOFTWARE PRODUCT, along with proof of payment, to the authorized dealer from whom you obtained the SOFTWARE PRODUCT for a full refund of the price you paid.

1. Ownership and License.
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD or its licensors. Your rights to use the SOFTWARE PRODUCT are as specified in this EULA, and WATCHGUARD retains all rights not expressly granted to you in this EULA. Nothing in this EULA constitutes a waiver of our rights under U.S. copyright law or any other law or treaty.

2. Permitted Uses.
You are granted the following rights to the SOFTWARE PRODUCT:
(A) You may use the SOFTWARE PRODUCT solely for the purpose of operating the SOHO hardware product in accordance with the SOHO or user documentation.
If you are accessing the SOFTWARE PRODUCT via a Web based installer program, you are granted the following additional rights to the SOFTWARE PRODUCT:
(A) You may install and use the SOFTWARE PRODUCT on any computer with an associated connection to the SOHO hardware product in accordance with the SOHO user documentation;
(B) You may install and use the SOFTWARE PRODUCT on more than one computer at once without licensing an additional copy of the SOFTWARE PRODUCT for each additional computer on which you want to use it, provided that each computer on which you install the SOFTWARE PRODUCT has an associated connection to the same SOHO hardware product ; and
(C) You may make a single copy of the SOFTWARE PRODUCT for backup or

archival purposes only.

3. Prohibited Uses.
You may not, without express written permission from WATCHGUARD:
(A) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT;
(B) Use, copy, modify, merge or transfer copies of the SOFTWARE PRODUCT or printed materials except as provided in this EULA;
(C) Use any backup or archival copy of the SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;
(D) Sublicense, lend, lease or rent the SOFTWARE PRODUCT; or
(E) Transfer this license to another party unless
(i) the transfer is permanent,
(ii) the third party recipient agrees to the terms of this EULA, and
(iii) you do not retain any copies of the SOFTWARE PRODUCT.

4. Limited Warranty.
WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer;
(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to us with a dated proof of purchase; and
(B) SOFTWARE PRODUCT. The SOFTWARE PRODUCT will materially conform to the documentation that accompanies it. If the SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return all of the SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and they will provide you with a new version of the SOFTWARE PRODUCT or a full refund at their election.

Disclaimer and Release.
THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD AND ITS LICENSORS, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THIS SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE SOFTWARE PRODUCT).

Limitation of Liability.
WATCHGUARD'S LIABILITY (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS WILL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.
IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS WILL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5. United States Government Restricted Rights.
The enclosed SOFTWARE PRODUCT and documentation are provided with Restricted Rights. Use, duplication or disclosure by the U.S Government or any agency or instrumentality thereof is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Incorporated, 505 5th Ave. South, Suite 500,Seattle, WA 98104.

6. Export Controls.
You agree not to directly or indirectly transfer the SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7. Termination.
This license and your right to use the SOFTWARE PRODUCT will automatically terminate if you fail to comply with any provisions of this EULA, destroy all copies of the SOFTWARE PRODUCT in your possession, or voluntarily return the SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the SOFTWARE PRODUCT and documentation remaining in your control or possession.

8. Miscellaneous Provisions. This EULA will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire EULA between us relating to the contents of this package, and supersedes any prior purchase order, communications, advertising or representations concerning the SOFTWARE PRODUCT
AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS EULA ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS EULA; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS EULA AND PERFORM ITS OBLIGATIONS UNDER THIS EULA AND; (C) THIS EULA AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS EULA DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY.

No change or modification of this EULA will be valid unless it is in writing, and is signed by WATCHGUARD.

WatchGuard Limited Hardware Warranty

This Limited Hardware Warranty (the "Warranty") applies to the enclosed WatchGuard hardware product (the "Product"), not including any associated software which is licensed pursuant to a seperate end-user license agreement and warranty. BY USING THE PRODUCT, YOU AGREE TO THE TERMS HEREOF. If you do not agree to these terms, please return this package, along with proof of purchase, to the authorized dealer from which you purchased it for a full refund. WatchGuard Technologies, Inc. ("WatchGuard") and you agree as follows:

1. Limited Warranty. WatchGuard warrants that upon delivery and for one (1) year thereafter (the "Warranty Period"): (a) the Product will be free from material defects in materials and workmanship, and (b) the Product, when properly installed and used for its intended purpose and in its intended operating environment, will perform substantially in accordance with WatchGuard applicable specifications.
This warranty does not apply to any Product that has been: (i) altered, repaired or modified by any party other than WatchGuard; or (ii) damaged or destroyed by accidents, power spikes or similar events or by any intentional, reckless or negligent acts or omissions of any party. You may have additional warranties with respect to the Product from the manufacturers of Product components. However, you agree not to look to WatchGuard for, and hereby release WatchGuard from any liability for, performance of, enforcement of, or damages or other relief on account of, any such warranties or any breach thereof.

2. Remedies. If any Product does not comply with the WatchGuard warranties set forth in Section 1 above, WatchGuard will, at its option, either (a) repair the Product, or (b) replace the Product; provided, that you will be responsible for returning the Product to the place of purchase and for all costs of shipping and handling. Repair or replacement of the Product shall not extend the Warranty Period. Any Product, component, part or other item replaced by WatchGuard becomes the property of WatchGuard . WatchGuard shall not be responsible for return of or damage to any software, firmware, information or data contained in, stored on, or integrated with any returned Products.

3. Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 1 AND 2 ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD OR FROM PRODUCT LIABILITY, STRICT LIABILITY OR OTHER THEORY, AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY,THE PRODUCT).

4. Limitation of Liability. WATCHGUARD TECHNOLOGIES' LIABILITY (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) WITH REGARD TO ANY PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF ANY AGREED REMEDY. IN NO

EVENT WILL WATCHGUARD TECHNOLOGIES BE LIABLE TO YOU OR ANY THIRD PARTY (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) FOR COST OF COVER OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF PROFITS, BUSINESS, OR DATA) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF WATCHGUARD TECHNOLOGIES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF ANY AGREED REMEDY.

5. Miscellaneous Provisions. This Warranty will be governed by the laws of the state of Washington, U.S.A., without reference to its choice of law rules. The provisions of the 1980 United Nations Convention on Contracts for the International Sales of Goods, as amended, shall not apply. You agree not to directly or indirectly transfer the Product or associated documentation to any country to which such transfer would be prohibited by the U.S. Export laws and regulations. If any provision of this Warranty is found to be invalid or unenforceable, then the remainder shall have full force and effect and the invalid provision shall be modified or partially enforced to the maximum extent permitted by law to effectuate the purpose of this Warranty. This is the entire agreement between WatchGuard and you relating to the Product, and supersedes any prior purchase order, communications, advertising or representations concerning the Product AND BY USING THE PRODUCT YOU AGREE TO THESE TERMS. No change or modification of this Agreement will be valid unless it is in writing, and is signed by WatchGuard.

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2002 WatchGuard Technologies, Inc. All rights reserved.
Firebox, Firebox 1000, Firebox 2500, Firebox 4500, Firebox II, Firebox II Plus, Firebox II FastVPN, Firebox III, Firebox SOHO, Firebox SOHO|tc, Firebox V100, Firebox V80, Firebox V60, Firebox V10, LiveSecurity, RapidStream, RapidCore, WatchGuard, WatchGuard Technologies, Inc., AppLock, AppLock/Web, Designing peace of mind, DVCP technology, Enforcer/MUVPN, FireChip, HackAdmin, HostWatch, LockSolid, RapidCare, SchoolMate, ServerLock, ServiceWatch, Smart Security. Simply Done., SpamScreen, Vcontroller are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries.

© Hi/fn, Inc. 1993, including one or more U.S. Patents: 4701745, 5016009, 5126739, and 5146221 and other patents pending.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT® and Windows® 2000 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

RC2 Symmetric Block Cipher, RC4 Symmetric Stream Cipher, RC5 Symmetric Block Cipher, BSAFE, TIPEM, RSA Public Key Cryptosystem, MD, MD2, MD4, and MD5 are either trademarks or registered trademarks of RSA Data Security, Inc. Certain materials herein are Copyright © 1992-1999 RSA Data Security, Inc. All rights reserved.

RealNetworks, RealAudio, and RealVideo are either a registered trademark or trademark of RealNetworks, Inc. in the United States and/or other countries.
Java and all Jave-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All right reserved.

© 1995-1998 Eric Young (eay@cryptsoft). All rights reserved.
© 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"
THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

© 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.
This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.
This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).
Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.
Copyright (c) 1998-2001 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."
4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Apache Software License, Version 1.1
Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:
"This product includes software developed by the Apache Software Foundation (http://www.apache.org/)."
Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.
Part No

Contents

CHAPTER 1 Introduction 1
The Package Contents 2
How Does a Firewall Work? 3
How Does Information Travel on the Internet? 4
IP addresses 4
Protocol 4
Port numbers 5
How Does the SOHO 6 Process Information? 5
Services 5
Network Address Translation 5
The SOHO 6 Hardware Description 6
The SOHO 6 front and rear views 6
CHAPTER 2 Installation 11
Before You Begin 12
Review and record your current TCP/IP settings 12

Disable the HTTP proxy setting of your Web browser 14
Enable your computer for DHCP 16
Physically connect the SOHO 6 18
Cabling the SOHO 6 for one to four appliances 19
Cabling the SOHO 6 for more than four computers . 20
CHAPTER 3 SOHO 6 Basics 23
The SOHO 6 Home Page—System Status 23
Default Factory Settings 25
Reset a SOHO 6 to factory default 26
The base model SOHO 6 27
Register your SOHO 6 and Activate the LiveSecurity Service 27
Reboot the SOHO 6 28
CHAPTER 4 Configure the Network Interfaces 31
Configure Your External Network 31
Network addressing 31
Configure the SOHO 6 External Network for dynamic addressing 32
Configure the SOHO 6 External Network for static addressing 33
Configure the SOHO 6 External Network for PPPoE 34
Configure the Trusted Network 36
Configure additional computers on the Trusted Network 36
Configure the Trusted Network with static addresses 37
Configure Static Routes 38

View Network Statistics 39
Configure the Dynamic DNS Service 40
CHAPTER 5 Administrative Options 43
The System Security Page 44
System management 44
SOHO Remote Management 46
Set up VPN Manager Access 46
Update Your Firmware 48
Redeem your SOHO 6 Upgrade Options 49
View the Configuration File 51
CHAPTER 6 Configure the Firewall Settings 53
Firewall Settings 53
Configure Incoming and Outgoing Services 54
Pre-configured Services 54
Create a Custom Service 55
Block External Sites 57
Firewall Options 59
Ping requests received on the External Network 60
Denying FTP access to the Trusted Network interface 60
SOCKS implementation for the SOHO 6 60
Logging all allowed outbound traffic 62
Create an Unrestricted Pass Through 63
CHAPTER 7 Configure Logging 65
View SOHO 6 Log Messages 66
Set up Logging to a WatchGuard Security Event Processor Log Host 67

Set up Logging to a Syslog Host 69
Set the System Time 70

CHAPTER 8 VPN—Virtual Private Networking 73
Why Create a Virtual Private Network? 73
What You Need 74
Enable the VPN Upgrade 76
Step-by-step Instructions for Configuring a SOHO 6 VPN Tunnel 76
Special Considerations 77
Frequently Asked Questions 77
MUVPN Clients 79
View the VPN Statistics 79

CHAPTER 9 SOHO 6 WebBlocker 81
How WebBlocker Works 81
Web site not in the WebBlocker database 82
Web site in the WebBlocker database 82
WatchGuard WebBlocker database unavailable 82
WebBlocker users and groups 83
Bypass the SOHO 6 WebBlocker 83
Purchase and Activate SOHO 6 WebBlocker 83
Configure the SOHO 6 WebBlocker 84
WebBlocker Categories 89
Search for Blocked Sites 92

CHAPTER 10 Support Resources 95
Troubleshooting Tips 95
General 95
Configuration 99

VPN Management 102
Contact Technical support 104
Online Documentation and In-Depth FAQs 104
Special Notices 104

Index 105

CHAPTER 1

Introduction

Welcome

Congratulations on purchasing the ideal solution for providing secure access to the Internet—the WatchGuard® Firebox® SOHO 6 or SOHO 6tc security appliance.

This User Guide is for both the SOHO 6 and the SOHO 6tc—the name SOHO 6 refers to both these appliances throughout this guide. The only difference between them is the ability to create and use a Virtual Private Network (VPN). The VPN option is added to the SOHO 6, while the SOHO 6 tc comes with the VPN option pre-installed.

Your new SOHO 6 provides peace of mind when connecting to the Internet using a high-speed cable or DSL modem, a leased line, or ISDN.

The most current installation and user information is available at the WatchGuard Web site:

http://support.watchguard.com/sohoresources/

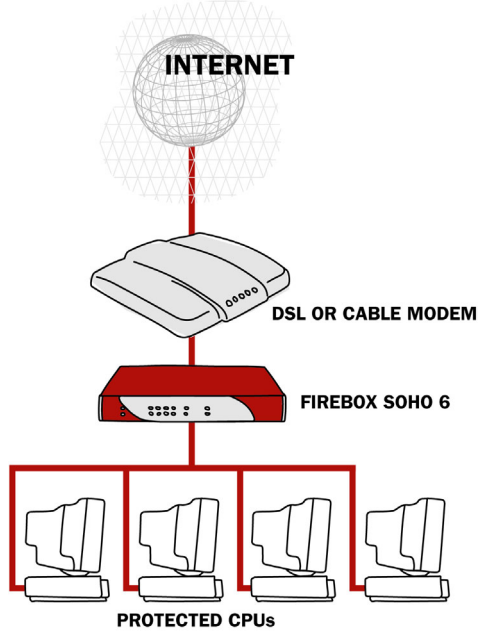
The Package Contents

First things first, check the package contents to make sure you have the following.

- *Firebox SOHO 6 QuickStart Guide*
- User documentation
- LiveSecurity Service® license key
- AC adapter (12v, 1.0-1.2A)
- Straight-through Ethernet cable
- SOHO 6 security appliance

How Does a Firewall Work?

Fundamentally, a firewall is a way of distinguishing between, as well as protecting, “us” and “them”. On the external side of your SOHO 6 firewall is the entire Internet. The Internet offers many resources such as the Web, email, and video/audio conferencing. It also presents dangers to the privacy and security of your computer. On the trusted side of your SOHO 6 firewall are all the appliances you want to protect from these dangers. As is illustrated in the image below, the SOHO 6 physically separates your trusted network from the Internet.



Using rules or policies outlined in Chapter 3: “Configure Incoming and Outgoing Services” on page 54, the WatchGuard SOHO 6 evaluates all traffic between the external network (the Internet)

and the trusted network (your computer) and blocks any suspicious activity.

How Does Information Travel on the Internet?

All information transported over the Internet is packaged in a special manner to ensure that it travels from one computer to the next. The program responsible for this task is known as TCP/IP. TCP (Transmission Control Protocol) manages the assembly and reassembly of data, for example an email message or program file, into smaller chunks of data called packets. IP (Internet Protocol) takes these packets and wraps them up with a header identifying both where the information is going and how it is handled en route.

IP addresses

An IP address defines the specific computer on the Internet that sends or receives a packet. Every computer on the Internet has a unique address, including your SOHO 6. When defining a service behind a firewall, you need to include the trusted, network address for the computer hosting the application.

On the Internet, IP addresses are identified using a string of numbers that have been translated from a URL (Uniform Resource Locator) name such as, www.watchguard.com.

Protocol

A protocol defines how a packet is bundled and packaged for shipment across a network. The most commonly used protocols are TCP and UDP (User Datagram Protocol). In addition, there are a variety of IP protocols that are less frequently used.

Port numbers

The port numbers are used by computers at both the sending and receiving end to determine the particular program or application for each connection.

How Does the SOHO 6 Process Information?

Services

A service is the combination of protocol(s) and port numbers associated with a specific program or application type. To simplify configuration of your SOHO 6, WatchGuard configured versions of several common services are available for your use.

Network Address Translation

All outgoing connections through a SOHO 6 automatically use a feature called dynamic NAT (Network Address Translation). Without dynamic NAT, your trusted, private addresses are passed along the Internet to their destination.

In addition, the SOHO 6 protects your trusted network by disguising private IP addresses. During an Internet connection, all traffic passed between computers includes IP address information. However, because of the dynamic NAT feature, applications and servers on the Internet only see the public, external IP address of the SOHO 6 itself and are never aware of the addresses in your trusted, network address range.

Imagine that you install a computer behind the SOHO 6 with the IP address 206.253.208.100. If this address were broadcast to the Internet, hackers could easily direct an attack on the computer itself. Instead, the SOHO 6 converts the address automatically to

the external address of the SOHO 6. When a hacker tries to violate the computer, they are stopped at the SOHO 6, never learning the true address of your computer.

The SOHO 6 Hardware Description

The SOHO 6 has significant improvements to the hardware platform from those of previous SOHO models.

Faster Processor

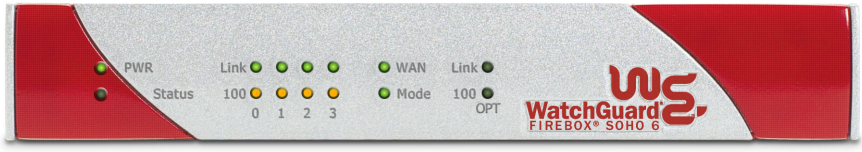
The SOHO 6 has a new network processor running at a speed of 150MHz. It also includes built in Ethernet and encryption technology.

Ethernet ports

The SOHO 6 has six 10/100 Base TX ports labeled OPT, WAN and numbered 0-3.

The SOHO 6 front and rear views

The SOHO 6 has fourteen indicator lights on the front panel of the appliance. The following photograph shows the entire front view.



PWR

When illuminated, this light indicates that the SOHO 6 is currently powered up.

Status

When illuminated, this light indicates that a management connection has been made.

Link

The link indicator illuminates when there is a good physical connection to any of the numbered (0-3) interfaces of the trusted network. The link indicator blinks when traffic is passing through the interface.

100

When a trusted network interface runs at 10Mb, the 100 indicator is *not* illuminated. When the network interface runs at 100 Mb, the 100 indicator is yellow.

WAN

Indicates a good physical connection to the external (WAN) port. The indicator blinks when traffic is passing through the interface.

Mode

Indicates that the SOHO 6 is operational and has connected to the Internet when illuminated.

The SOHO 6 has six Ethernet ports, a reset button, and a power input located on the rear of the appliance. The following photograph shows the entire rear view.

OPT port

The Ethernet port labeled OPT is currently disabled.

RESET button

Using the reset button, you can return to the SOHO 6 to the factory defaults. For more information on performing this function, see "Reset a SOHO 6 to factory default" on page 26.

WAN port

This Ethernet port corresponds to the external interface.

4 numbered ports (0-3)

These Ethernet ports correspond to the trusted interface.

Power input

Accepts the 12 volt AC adapter supplied with the SOHO 6.

CHAPTER 2

Installation

This chapter explains how to install the SOHO 6 into your network. You must complete the following steps:

- Review and record your current TCP/IP settings
- Disable the HTTP proxy setting of your Web browser
- Enable your computer for DHCP
- Physically connect the SOHO 6 to your network

For a quick summary of this information, see the *Firebox SOHO 6 QuickStart Guide* included with your SOHO 6.

Before You Begin

Before installing your new SOHO 6, be certain that you have the following items:.

- A 10/100BaseT Ethernet I/O network card installed in your computer.
- A cable or DSL modem with a 10/100BaseT port or an ISDN router. This is unnecessary if you connect to the Internet using a LAN connection.
- Two Ethernet network cables with RJ45 connectors. These must *not* be "crossover cables" (often red or orange). One cable is furnished with your SOHO 6. Make certain that both cables are long enough to comfortably connect the modem or router to the SOHO 6 and the SOHO 6 to your computer.
- A functioning Internet connection. If your connection does not work, please contact your ISP (Internet Service Provider).
- Call your ISP to find out which method they use to issue your newtork addressing—static addresses, DHCP, or PPPoE. You need this information later in the installation process, see "Configure Your External Network" on page 31.
- An installed Web browser—either Netscape Navigator 4.77 (or higher) or Internet Explorer 5.0 (or higher).
- The SOHO 6 serial number.

Review and record your current TCP/IP settings

For your reference, record the computer's current TCP/IP settings in the chart at the end of this section. Access to this information depends on your computer operating system.

Microsoft Windows 2000

1 Click **Start ⇒Programs ⇒Accessories ⇒Command Prompt**.

2 At the default prompt, type `ipconfig/all`, then press **Enter**.
3 Enter the TCP/IP settings in the chart provided below.
4 Click **Cancel**.

Microsoft Windows NT

1 Click **Start** ⇒**Programs** ⇒**Command Prompt**.
2 At the default prompt, type `ipconfig/all`, then press **Enter**.
3 Enter the TCP/IP settings in the chart provided below.
4 Click **Cancel**.

Microsoft Windows 95 or 98 or ME

1 Click **Start** ⇒**Run**.
2 Type: `winipcfg`. Click **OK**.
3 Select the "Ethernet Adapter."
4 Enter the TCP/IP settings in the chart provided below.
5 Click **Cancel**.

Macintosh

1 Click the **Apple** menu ⇒**Control Panels** ⇒**TCP/IP**.
2 Enter the TCP/IP settings in the chart provided below.
3 Close the window.

Other operating systems (Unix, Linux)

1 Consult your operating system guide to locate the TCP/IP screen.
2 Enter the settings in the chart provided below.

3 Exit the TCP/IP configuration screen.

TCP/IP Setting		Value
IP Address		. . .
Subnet Mask		. . .
Default Gateway		. . .
DHCP Enabled		Yes No
DNS Server(s)	Primary	. . .
	Secondary	. . .

NOTE

If you are connecting more than one computer to the trusted network behind the SOHO 6, determine the TCP/IP settings for each computer.

Disable the HTTP proxy setting of your Web browser

To configure a SOHO 6 after it is installed, you must access the special configuration pages that reside on the SOHO 6. If the HTTP proxy setting in your browser is enabled, you cannot access these pages, making it impossible to complete the configuration process.

With the HTTP proxy enabled, the browser automatically points itself to Web pages located on the Internet, and you cannot direct the browser to Web pages located in other places. Disabling the HTTP does not prevent you from accessing your favorite Web sites, but it does allow you to access the configuration pages that reside on the SOHO 6.

To disable the HTTP proxy in three commonly used browsers, see the instructions below. If your browser is not listed, see your browser Help menus to learn how to disable the HTTP proxy settings.

Netscape 4.7

1 Open Netscape.

2 Click **Edit ⇒Preferences**.
The Preferences window appears.

3 From among the categories listed on the left hand side of the window, click the **+** symbol before the **Advanced** heading to expand the list.

4 Click **Proxies**.

5 Verify that the **Direct Connection to the Internet** option is enabled.

6 Click **OK** to save the settings.

Netscape 6.x

1 Open Netscape.

2 Click **Edit ⇒Preferences**.
The Preferences window appears.

3 From among the categories listed on the left side of the window, click the arrow symbol before the **Advanced** heading to expand the list.

4 Click **Proxies**.

5 Verify that the **Direct Connection to the Internet** option is active.

6 Click **OK** to save the settings.

Internet Explorer 5.0, 5.5, and 6.0

1 Open Internet Explorer.

2 Click **Tools ⇒ Internet Options**.
The Internet Options window appears.

3 Click the **Advanced** tab.

4 Scroll down the page to **HTTP 1.1 Settings**.

5 Disable all checkboxes.

6 Click **OK** to save the settings.

Enable your computer for DHCP

In order to access the special configuration pages on the SOHO 6 after you have physically connected it, your computer must be configured to receive it's network IP address by DHCP. For more information regarding network addressing as well as DHCP, see "Network addressing" on page 31.

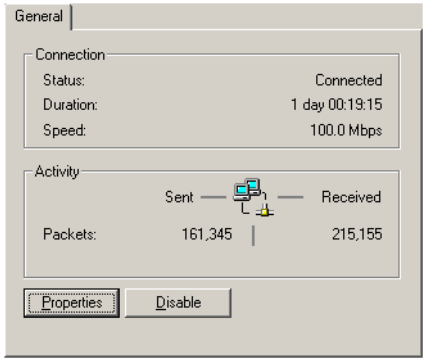
NOTE

The configuration instructions in this section are for the Windows 2000® operating system.

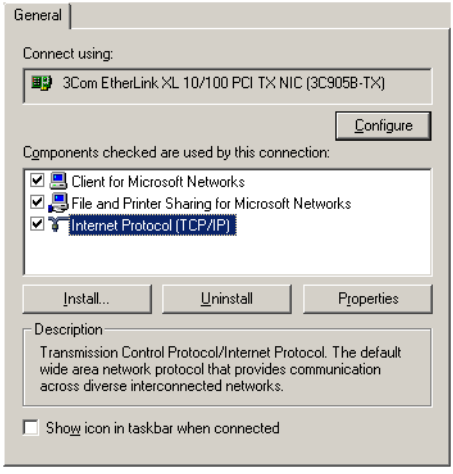
1 Click **Start ⇒Settings ⇒Control Panel**.
The Control Panel window appears.

2 Double-click the **Network & Dial-up Connections** icon.

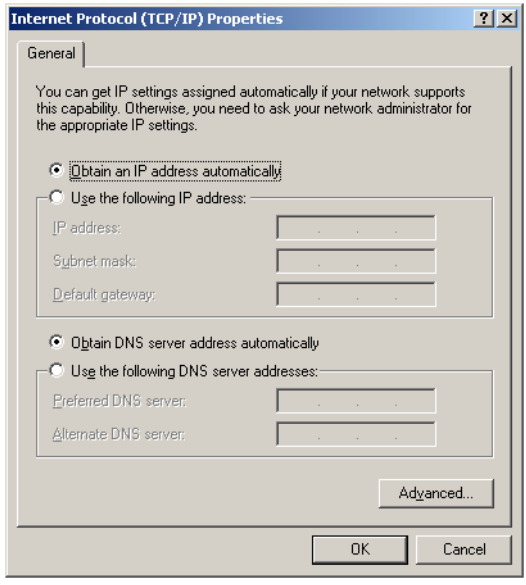
3 Double-click on the connection you use to access the Internet.
The network connection dialog box appears.



4 Click **Properties**.
The network connection Properties dialog box appears.


General
Connect using:
3Com EtherLink XL 10/100 PCI TX NIC (3C905B-TX)
Configure
Components checked are used by this connection:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in taskbar when connected

5 Double click the **Internet Protocol (TCP/IP)** component.
The Internet Protocol (TCP/IP) Properties dialog box appears.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 Select **Obtain an IP address automatically**. Select **Obtain DNS server address automatically**.

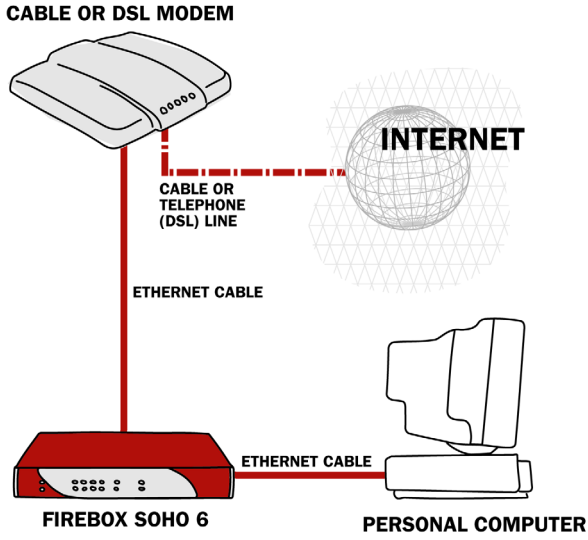
7 Click **OK** to close the Internet Protocol (TCP/IP) Properties dialog box. Click **OK** again to close the network connection Properties dialog box. Click **Close** to close the network connection dialog box. Close the Control Panel window.

Physically connect the SOHO 6

Your SOHO 6 protects a single computer or a multi-computer network. It also functions as a hub to connect a variety of other appliances.

Cabling the SOHO 6 for one to four appliances

Each of the Trusted Network ports (numbered 0-3) is able to connect to a variety of appliances. These include computers, printers, scanners, or other network peripherals. Use your SOHO 6 to replace an existing hub if you have no more than four appliances to connect.



1 Shut down your computer. If you connect to the Internet using a DSL/cable modem, disconnect the power from this device

2 Disconnect the Ethernet cable that runs from your DSL/cable modem or other Internet connection to your computer and connect it to the WAN port on the SOHO 6.

The SOHO 6 is now connected directly to the modem or other Internet connection.

3 Connect one end of the straight-through Ethernet cable supplied with your SOHO 6 into any one of the four,

numbered, Ethernet ports (labeled 0-3) on the SOHO 6. Connect the other end into the Ethernet port of your computer.
The SOHO 6 is now connected to the Internet and your computer.

4 If you connect to the Internet using a DSL/cable modem, restore the power to this device. When the indicator lights of the modem stop flashing the modem is ready for use.

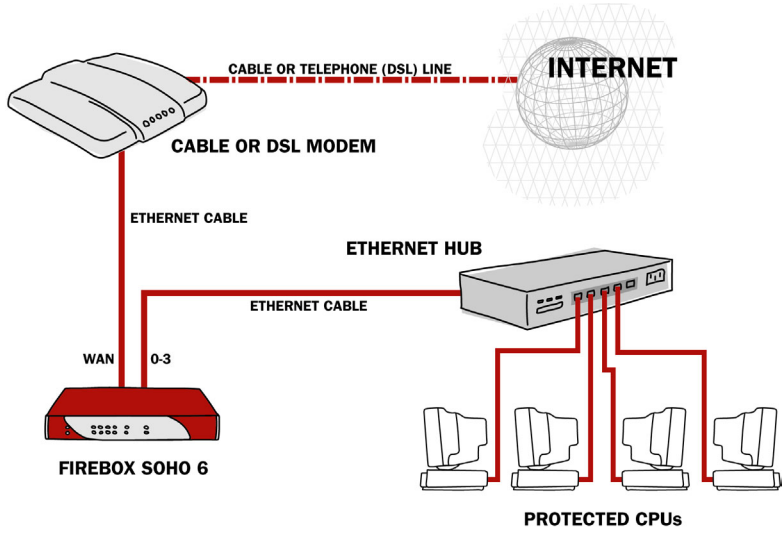
5 Attach the AC adapter to the SOHO 6 and connect it to a power source.

6 Restart your computer.

For information on the factory default configuration options, see "Default Factory Settings" on page 25. For specialized configurations, see "Configure Your External Network" on page 31, as well as, "Configure the Trusted Network" on page 36.

Cabling the SOHO 6 for more than four computers

While there are only four, numbered, Ethernet ports (labeled 0-3) on the back of the SOHO 6, it is possible to connect more appliances to your SOHO 6 using network hubs.



The SOHO 6 ships with a "10-seat" license. In other words, the SOHO 6 allows up to ten computers on a network behind the SOHO 6 to access the Internet. More than ten computers can exist on the network and communicate with each other, but only the first ten that attempt to access the Internet are allowed through the SOHO 6. A seat is taken when a computer connects to the Internet. To upgrade your SOHO 6 user license, please visit:

http://www.watchguard.com/sales/buyonline.asp

You need these additional items:

- One or more Ethernet hubs.
- An Ethernet cable (with RJ-45 connectors) for each computer to connect to the SOHO 6.
- An Ethernet cable to connect each hub to the SOHO 6.

1 Shut down your computer. If you connect to the Internet using a DSL/cable modem, disconnect the power from this device

2 Disconnect the Ethernet cable that runs from your DSL/cable modem or other Internet connection to your computer and connect it to the WAN port on the SOHO 6.
The SOHO 6 is now connected directly to the modem or other Internet connection.

3 Connect one end of the straight-through Ethernet cable supplied with your SOHO 6 into any one of the four, numbered, Ethernet ports (labeled 0-3) on the SOHO 6. Connect the other end into the uplink port of the hub.
The SOHO 6 is now connected to the Internet and your hub.

4 Connect Ethernet cables to the uplink ports of the hub and to the Ethernet ports of each of your computers.

5 If you connect to the Internet using a DSL/cable modem, restore the power to this device. When the indicator lights of the modem stop flashing the modem is ready for use.

6 Attach the AC adapter to the SOHO 6 and connect it to a power source.

7 Restart your computer.

For information on the factory default configuration options, see "Default Factory Settings" on page 25. For specialized configurations, see "Configure Your External Network" on page 31, as well as, "Configure the Trusted Network" on page 36.

CHAPTER 3

SOHO 6 Basics

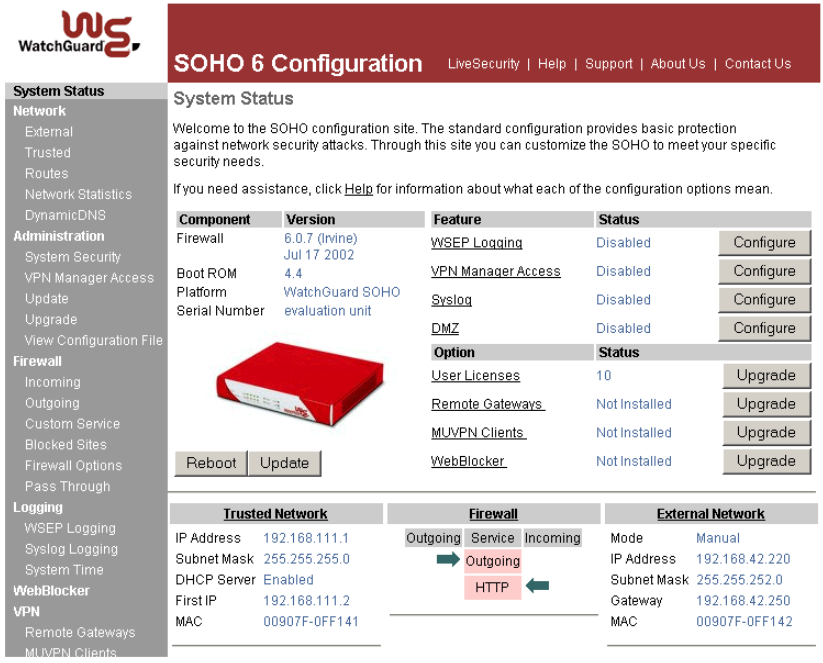
Once you have physically installed the SOHO 6, you can connect to it using your Web browser. The SOHO 6 includes a Web server that provides a configuration, Web page interface.

The SOHO 6 Home Page—System Status

With your Web browser, go to the System Status page of the SOHO 6 using the default IP address of the Trusted Network:

http://192.168.111.1.

The System Status page appears.



The System Status page is effectively the home page of the SOHO 6. A variety of information is revealed in an effort to provide a comprehensive display of the SOHO 6 configuration. This information includes:

- The firmware version
- The serial number of the appliance
- A few of the SOHO 6 features and their status:
  - WSEP Logging
  - VPN Manager
  - Syslog

  - Pass Through
  - DHCP Release/renew
- Upgrade options and their status
- Configuration information for both the Trusted and External networks

NOTE

When the External network is configured to use the PPPoE Client, the page also displays a connect or disconnect button in order to terminate or initiate the PPPoE connection.

- Configuration information on firewall settings (Incoming and Outgoing services)
- A reboot button to restart the SOHO 6

Default Factory Settings

Your SOHO 6 has the following default network and configuration settings:

External Network

External network settings use DHCP.

Trusted Network

The trusted network IP address is 192.168.111.1.

All computers on the trusted network automatically receive their addresses using DHCP.

Firewall Settings

All incoming services are blocked.

An outgoing service allowing all outbound traffic.

None of the Firewall Options are enabled.

The DMZ pass-through is disabled.

System Security

System Security is disabled and no System Administrator name or passphrase is set—the configuration pages are available to all on the trusted network.

SOHO 6 Remote Management is disabled.

VPN Manager Access is disabled.

No remote logging is configured.

WebBlocker

WebBlocker is disabled and no settings are configured.

Upgrade Options

No upgrade options are enabled until the license keys are redeemed.

Reset a SOHO 6 to factory default

Firmware corruptions or other unforeseen events (such as a lost System Security passphrase) require you to reset the SOHO 6 to its factory default settings.

To do this, first disconnect the power supply. Then find the reset button located at the rear of the SOHO 6. Press and hold the reset button. At the same time, reconnect the power supply. Continue pressing the reset button while the SOHO 6 reboots—approximately 15 seconds. The PWR indicator light should blink in a steady pattern once the reboot is complete. When this occurs, reboot the SOHO 6 again by disconnecting the power supply.

Finally, the PWR indicator light should remain illuminated. Your SOHO 6 is now reset to factory defaults.

The base model SOHO 6

The base model SOHO 6 comes with a ten-seat license; that is, ten computers have access to the Internet through the SOHO 6. Remember, while only four appliances connect directly to the four (numbered 0-3) Ethernet ports, one or more of these appliances can be a hub or router. Please see, "Cabling the SOHO 6 for more than four computers" on page 20.

Register your SOHO 6 and Activate the LiveSecurity Service

Once the SOHO 6 is installed and configured, you need to register the unit and activate your bundled LiveSecurity Service subscription. Activation entitles you to receive threat alert notifications, expert security advice, free anti-virus protection, software updates, technical support by web or phone, and access to extensive online help resources and our user forum. You must also activate to retrieve feature keys for any upgrades you have purchased.

Be sure that you have the SOHO 6 serial number handy. You will need this during the registration process.

To register with the LiveSecurity Service:

1 Using your Web browser, go to:

http:\\www.watchguard.com\activate

NOTE

You *must* have JavaScript enabled on your browser to be able to activate LiveSecurity Service.

If you are a returning customer, log in with your user name and password then choose your product and continue by following the instructions on screen.

If you are a new WatchGuard customer, begin by creating a profile, then follow the instructions on screen for activating a product.

Please use the table below to record your LiveSecurity Service identification information:

Serial Number:	
LiveSecurity User Name:	
Password:	

The SOHO 6 serial number is located on the bottom of the appliance. You create a LiveSecurity Service user name and password when you register your SOHO 6.

Please keep this information in a secure place.

Reboot the SOHO 6

To reboot a SOHO 6 located on a local system, use one of these methods:

- With your Web browser, go to the System Status page using the trusted IP address of the SOHO 6. For example, if using

the default IP address, go to: http://192.168.111.1. Click **Reboot**.

- Unplug the SOHO 6 and reconnect it to a power source.

To reboot a SOHO 6 located on a remote system, you must set the SOHO 6 to allow either incoming HTTP (Web) or FTP traffic to the trusted address of the SOHO 6. For information on configuring a SOHO 6 to allow incoming traffic, see "Configure Incoming and Outgoing Services" on page 54.

You then use one of these methods:

- With your Web browser, go to the System Status page using the external IP address of the SOHO 6. Click **Reboot**.
- Send an FTP command to the remote SOHO 6. Use an FTP application to connect to the SOHO 6, then enter the command: `quote rebt`

CHAPTER 4

Configure the Network Interfaces

Configure Your External Network

When you configure the external network, you establish how the SOHO 6 communicates with your ISP. This configuration depends upon how your ISP distributes network addresses—using DHCP or PPPoE.

Network addressing

Each networked computer must have an IP address to identify itself to other computers. IP address assignments are either dynamic or static. With a dynamic IP address, your ISP assigns each computer a different address each time it connects to the server. When you power down the computer, you release that IP address allowing it to be reassigned. A static IP address is assigned to your computer at all times whether or not you are currently using it. No other computer on the network shares that address.

The most common method to distribute IP addresses is dynamically using DHCP (Dynamic Host Configuration Protocol). When your computer is connected to the network, a DHCP server at your ISP automatically assigns it a network IP address. This relieves the ISP of the responsibility to manually assign and manage individual IP addresses.

Another method of dynamically assigning IP addresses is called PPPoE (Point-to-Point Protocol over Ethernet). PPPoE combines some of the advantages of Ethernet and PPP by simulating a standard dial-up connection. It is popular among many ISPs because it allows them to use their existing dial-up infrastructure such as billing, authentication, and security for DSL and cable modems. When configured to use PPPoE, the connection can be manually connected or disconnected from the System Status page.

Contact your ISP to determine which method they use to assign your IP address.

Configure the SOHO 6 External Network for dynamic addressing

The SOHO 6 is configured to obtain its external address information automatically using DHCP. If your ISP supports this method, the SOHO 6 obtains all necessary address information when it powers on and attempts to connect to the Internet. No further configuration of the SOHO 6 is required.

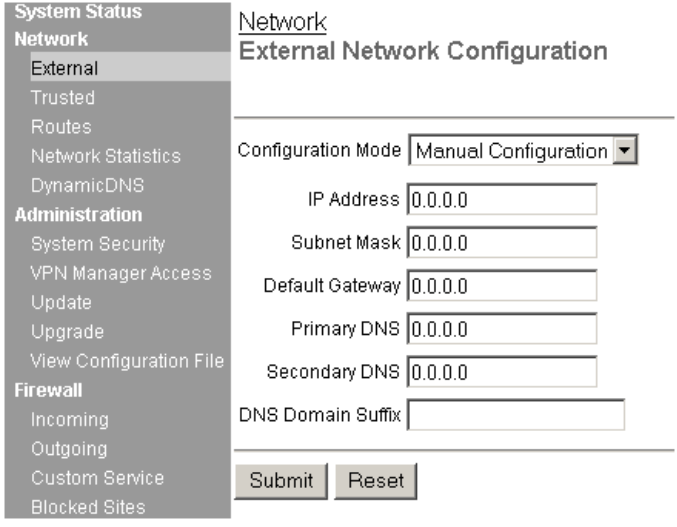
Configure the SOHO 6 External Network for static addressing

If you are assigned a static address, then you must transfer the permanent address assignment from your computer to the SOHO 6. Instead of communicating directly to your computer, the ISP now communicates through the SOHO 6.

1 With your Web browser, go to the System Status page using the trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Network ⇒External**.
The External Network Configuration page appears.

3 From the Configuration Mode drop list, select **Manual Configuration**.
The page refreshes.



4 Enter the TCP/IP settings you recorded from your computer during the installation process. Refer to the table in, "Review and record your current TCP/IP settings" on page 12.

5 Click **Submit**.
The configuration change is saved to the SOHO 6.

Configure the SOHO 6 External Network for PPPoE

While less common, PPPoE is another method for an ISP to assign IP addresses. Check the information and manuals sent to you by your ISP to see if they use PPPoE. If you cannot find this information, contact your ISP and ask them. You need your PPPoE login name and password.

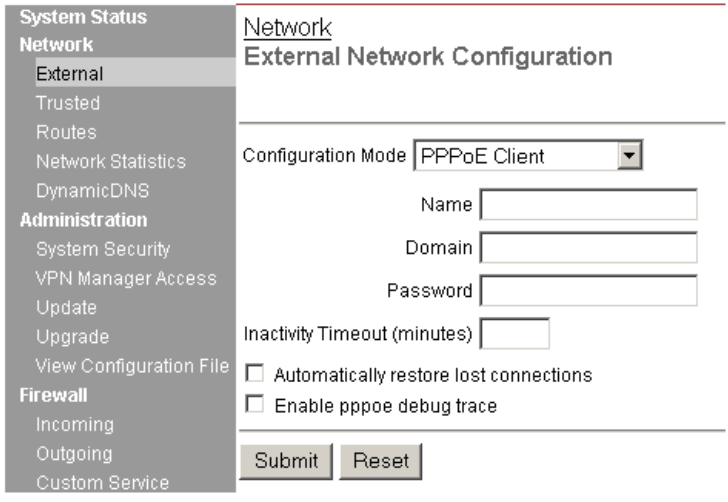
To configure the SOHO 6 for PPPoE:

1 Open your Web browser and click **Stop**.
At this point, the Internet connection is not fully configured, and the computer cannot load your home page from the Internet. However, the computer can access the configuration Web pages installed on the SOHO 6.

2 With your Web browser, go to the System Status page using the trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

3 From the navigation bar on the left side, select **Network ⇒ External**.
The External Network configuration page appears.

4 From the Configuration Mode drop list, select **PPPoE Client**.
The page refreshes.



5 Enter the PPPoE login name supplied by your ISP.

6 Enter the PPPoE password supplied by your ISP

7 Click **Automatically restore lost connections.**
This enables a constant flow of "heartbeat" traffic between the SOHO 6 and the PPPoE server. In the event of routine packet loss, this option allows the SOHO 6 to maintain the PPPoE connection. The SOHO 6 may reboot to recover this connection if the heartbeat fails. This provides for a more consistent Internet connection and is seen as continuous traffic by the ISP and regulated (and in some cases billed) as such. This option is also used for Technical Support debugging purposes.

8 Click **Submit**.
The configuration change is saved to the SOHO 6.

Configure the Trusted Network

By default, the SOHO 6 uses DHCP to assign addresses to computers on your trusted network. In other words, every time you connect a computer to the SOHO 6, either directly or through a hub, it automatically attempts to obtain its addresses from the SOHO 6.

Configure additional computers on the Trusted Network

The SOHO 6 accepts connections from up to four computers. Network a larger number of computers together using one or more 10BaseT Ethernet hubs with RJ-45 connectors. The SOHO 6 system coexists with other systems over the same LAN (Local Area Network). If you mix computers with different operating systems on your network they pass traffic through the SOHO 6 to access the Internet.

Follow these steps to add one or more computers to your Trusted network:

1 Verify that each additional computer has an Ethernet card installed. Shut the computer down, connect it to the network the same way you did in "Cabling the SOHO 6 for more than four computers" on page 20. Restart the computer.

2 Set the computers to obtain their addresses using DHCP. For instructions see, "Enable your computer for DHCP" on page 16.

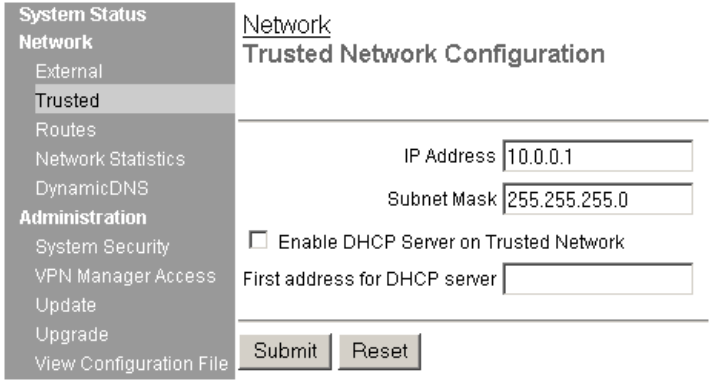
3 Turn off and restart each computer.

Configure the Trusted Network with static addresses

To disable the SOHO 6 DHCP server and assign addresses statically, follow these steps:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Network ⇒ Trusted**.
The Trusted Network Configuration page appears.



3 Enter the IP address and the Subnet Mask in the appropriate fields.

4 Disable the checkbox labeled **Enable DHCP Server on the Trusted Network**.

5 Click **Submit** and reboot the SOHO 6 as necessary.

6 Configure your computers and other devices on the trusted network with static addresses.

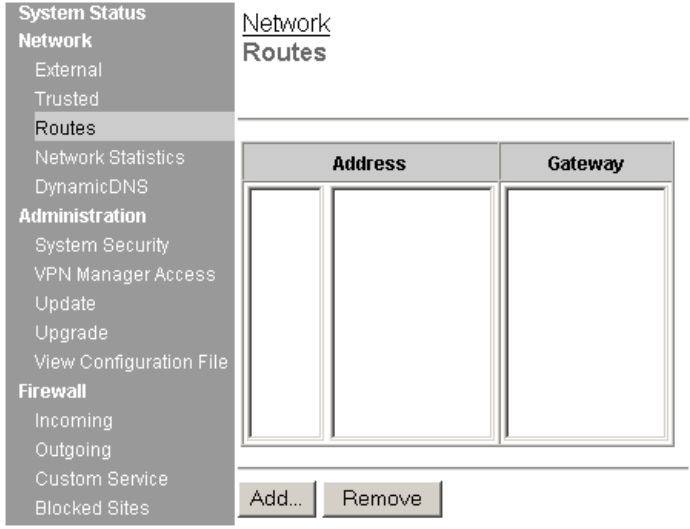
Configure Static Routes

The SOHO 6 allows you to configure static routes in order to pass traffic to networks on separate segments. This means that the SOHO 6 can route data packets to additional networks connected to a router or switch behind the SOHO 6.

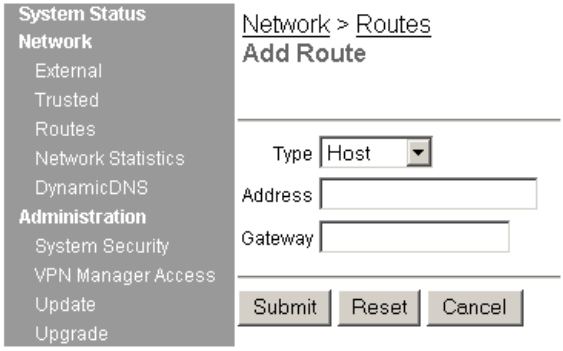
Follow these instructions to configure static routes:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Network ⇒ Routes**.
The Routes page appears.



3 Click **Add**.
The Add Route page appears.



4 From the Type drop list, select either **Host** or **Network**.

5 Enter the IP address and the Gateway of the route in the appropriate field.
The gateway of the route is the local interface of the router.

6 Click **Submit**.

To remove a route, select the appropriate entry and click **Remove**.

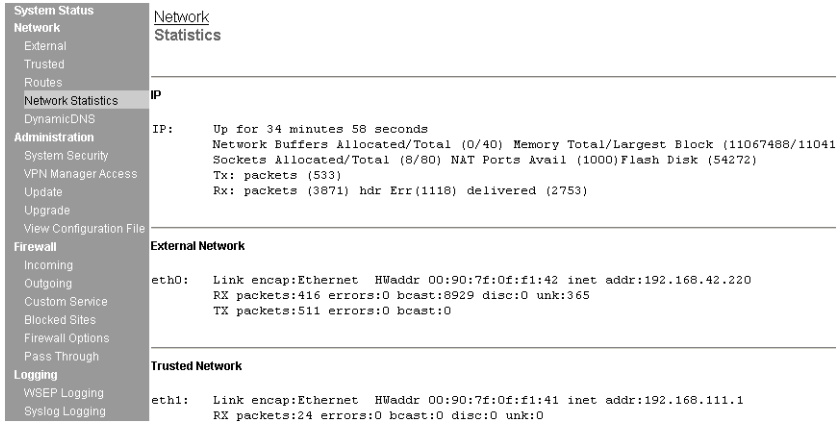
View Network Statistics

The SOHO 6 has a configuration page that displays a variety of network statistics to assist in monitoring data traffic as well as troubleshooting potential problems.

Follow these instructions to view this page:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Network ⇒ Network Statistics**.
The Network Statistics page appears.



Configure the Dynamic DNS Service

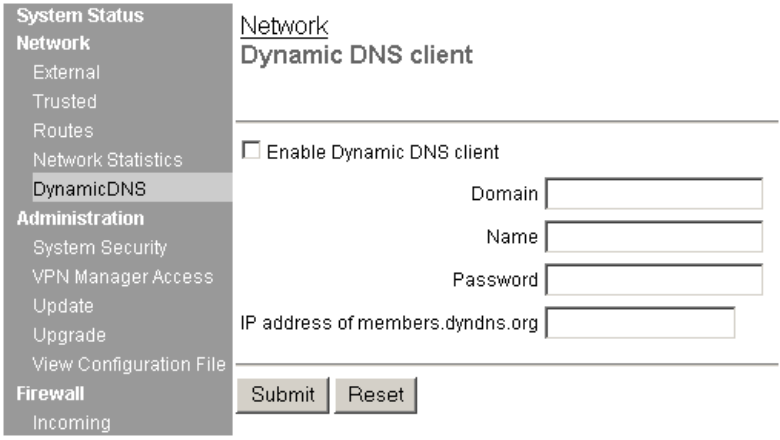
This feature allows you to register the external, IP address of the SOHO 6 with a dynamic DNS (Domain Name Server) service (www.dyndns.org). This service allows customers to bind their DNS record in the event that their dynamically assigned IP address is reassigned.

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

NOTE

WatchGuard is not affiliated with dyndns.org.

2 From the navigation bar on the left side, select **Network ⇒ DynamicDNS**.
The Dynamic DNS client page appears.



3 Select the **Enable Dynamic DNS client** checkbox.

4 Enter the domain, name, password, and the IP address of members.dyndns.org in the appropriate fields.

NOTE

THe SOHO 6 receives the IP of members.dyndns.org when it connects to the time server.

5 Click **Submit**.

CHAPTER 5

Administrative Options

The SOHO 6 Administration page is where you configure access to the SOHO 6—using System Security, enabling SOHO 6 Remote Management, or providing VPN Manager Access. You can also update the firmware, enter the feature key for any upgrade options you have purchased and have redeemed at the LiveSecurity Service Web site, as well as see the SOHO 6 configuration file in a text format.

The System Security Page

The System Security configuration page allows you to create secure settings to protect the configuration of the SOHO 6. Setting a system administrator name and system passphrase allows you to protect the SOHO 6 by using a simple authentication method.

This page also allows you to create a secure connection, using IPSec (Internet Protocol Security), to the SOHO 6 from a remote location.

System management

Passphrases are a barrier between your computer and anyone trying to break in. They are the first line of defense in computer security. They are, unfortunately, the most frequently overlooked of all security measures. The SOHO 6 system administrator name and system passphrase are designed to protect the SOHO 6 configuration from alteration by someone on your trusted network. In other words, when you configure a SOHO 6 system administrator name and system passphrase, no one in your office is able to change (deliberately or accidentally) your firewall settings without the proper passphrase.

NOTE

Make certain that you do not lose this name and passphrase. Once system security protection is activated, there is no other means of accessing your SOHO 6 settings. Should you forget your name or passphrase, the only means of accessing the appliance requires reverting your SOHO 6 to its factory settings; see "Reset a SOHO 6 to factory default" on page 26, you will then need to reconfigure your SOHO 6.

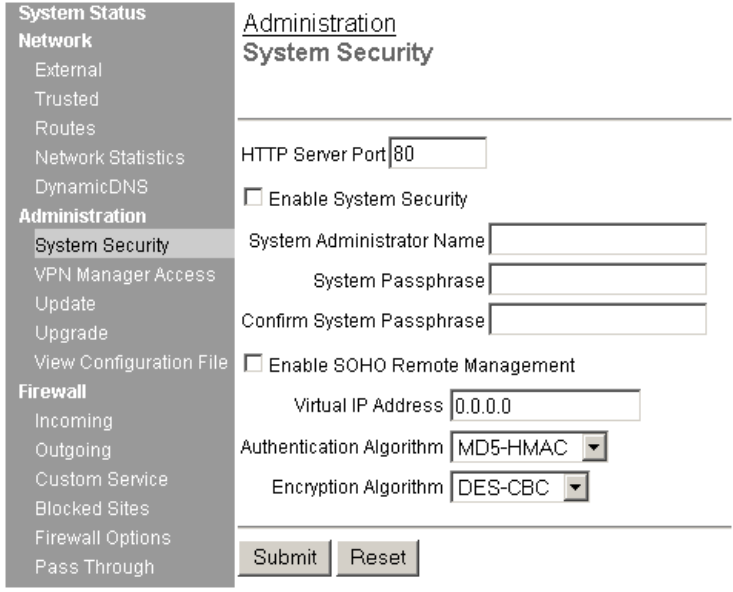
Change the system passphrase at least monthly. A passphrase (eight characters long) is a combination of letters, numbers, and symbols that do not spell out common words. WatchGuard

recommends that the passphrase contain at least one special character, number, and a mixture of upper and lower case letters for increased security.

Follow these steps to setup the SOHO 6 System Passphrase:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1.

2 From the navigation bar on the left side, select **Administration ⇒ System Security**.
The System Security page appears.



3 Verify that the HTTP Server Port is set at 80.

4 Select the **System Security** checkbox.

5 Enter the System Administrator Name.

6 Enter the System Passphrase and confirm it.

7 Click **Submit**.

SOHO Remote Management

This page also allows you to create a secure connection, using Internet Protocol Security (IPSec), to the SOHO from a remote location: SOHO Remote Management. This feature is discussed at length in the *Firebox SOHO 6 Remote Management Guide* located on our Web site at:

http://help.watchguard.com/documentation/soho.asp

Set up VPN Manager Access

The SOHO 6 works with WatchGuard VPN Manager software access in order to configure and manage Branch Office VPN tunnels from a remote location.

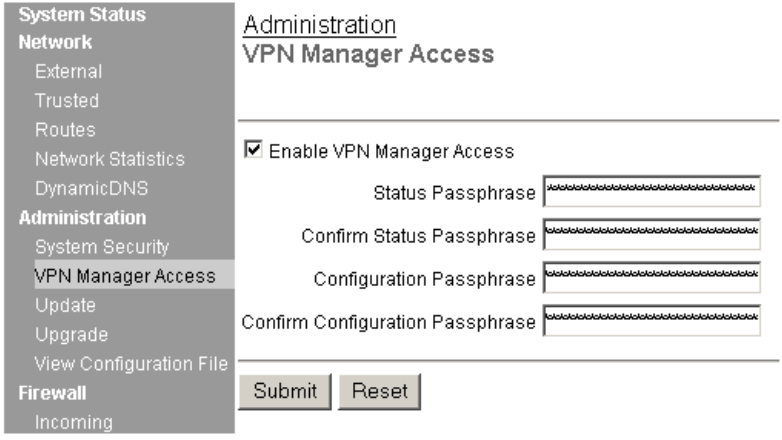
VPN Manager software is purchased separately and must run on a WatchGuard Firebox II/III. For more information regarding the VPN Manager product, use your Web browser to go to:

https://www.watchguard.com/products/vpnmanager.asp

Follow these steps to setup VPN Manager access:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Administration ⇒VPN Manager Access**.
The VPN Manager Access page appears.



3 Select **Enable VPN Manager Access**.

4 Enter the status passphrase and confirm it.

5 Enter the configuration passphrase and confirm it.

NOTE

These two settings *must* exactly match the passphrases used in the VPN Manager or the connection will fail.

6 Click **Submit**.

Update Your Firmware

As new firmware is released, you should update the version running on your SOHO 6. New updates are located on the WatchGuard Web site at:

http://support.watchguard.com/sohoresources/

Download the new firmware file from the Web site and save it to a known location on your management station.

Once you have downloaded the firmware, follow these steps to update the version running on your SOH O 6:

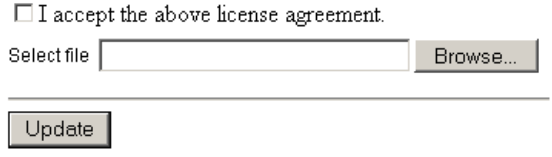
1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Administration ⇒Update**.
The Update page appears.

NOTE

If you are managing your SOHO 6 from a computer running an operating system other than Windows (such as a Macintosh or Linux OS), you *must* update your firmware from this configuration page as firmware versions are released. This is because WatchGuard installation applications are only built for Windows platforms.

3 Read through the End-User License Agreement, then select the **I accept the above license agreement** checkbox at the bottom of the page.



4 Enter the location of the firmware files located on your computer.

5 If you do not know the location of the firmware files, click **Browse** to browse your computer's directories and select them.

6 Click **Update**.
Follow the instructions provided by the Update Wizard.

NOTE

The Update Wizard will request a User name and Password. These values correspond System Administrator Name and System Passphrase configured at the System Security page. The default values are User and Pass.

Redeem your SOHO 6 Upgrade Options

When you purchase a SOHO 6, the software for all upgrade options is provided with the unit regardless of whether you have actually purchased any of those options. The Feature Key that enables these software options is stored within the SOHO 6. Once you purchase an upgrade option and redeem it at the LiveSecurity Service Web site, you will receive a Feature Key, which you can then copy and paste into a SOHO 6 configuration page, to activate the software upgrade.

For information on registering your SOHO 6 with the LiveSecurity Service, see "Register your SOHO 6 and Activate the LiveSecurity Service" on page 27.

Follow these steps to redeem your upgrade option license key:

1 With your Web browser, go to:
http://www.watchguard.com/upgrade

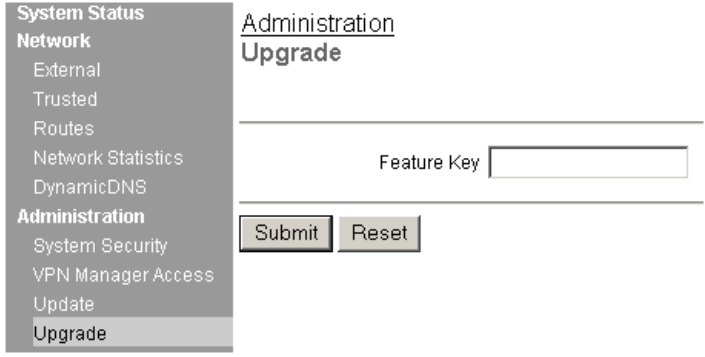
2 Click the **LiveSecurity** link at the top of the page and log into the site.

3 Follow the instructions provided on the site to redeem your upgrade license key.

4 Copy the Feature Key displayed at the LiveSecurity Service Web site.

5 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

6 From the navigation bar on the left side, select **Administration ⇒Upgrade**.
The Upgrade page appears.



7 Paste the Feature Key in the appropriate field.

8 Click **Submit**.

Upgrade options

Seat Licenses

This upgrade to the SOHO 6 provides more seats than the base model offers (for example, the 25 seat license).

IPSec Virtual Private Networking (VPN)

The SOHO 6tc comes with a VPN upgrade license key. You must activate the VPN upgrade in order to configure virtual private networking. The SOHO 6 does not come with the VPN upgrade license key. This license key is purchased separately.

WebBlocker

The SOHO 6 has a Web filtering option. This license key is purchased separately.

MUVPN Clients

With this upgrade the SOHO 6 allows remote users to securely connect to it through an IPSec VPN and access network resources on the Trusted network. These license keys are purchased separately.

LiveSecurity Service Subscription Renewals

Subscription renewals are available for a period of one or two years and may be purchased from your reseller or from the WatchGuard online store. To purchase renewals online or activate a renewal certificate, visit:

http://www.watchguard.com/renew/

Follow the instructions at the site to activate or purchase the renewal.

View the Configuration File

From this configuration page, the SOHO 6 configuration file appears in text format.

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Administration ⇒View Configuration File**.
The View Configuration File page appears.

CHAPTER 6

Configure the Firewall Settings

Firewall Settings

The flow of incoming and outgoing traffic is controlled by the configuration setting you make. These decisions are made in accordance with a sound security policy that defines the kinds of risks that are acceptable to you or your firm.

WatchGuard identifies several commonly used services that are used to define incoming and outgoing access. A service is the combination of protocol and port numbers associated with a specific application or communication type.

Configure Incoming and Outgoing Services

By default, the security stance of the SOHO 6 is to deny incoming packets to computers on the trusted network protected by the SOHO 6 firewall. You can selectively open your network to certain types of Internet connectivity. For example, to set up a Web server behind the SOHO 6, you add an incoming Web service.

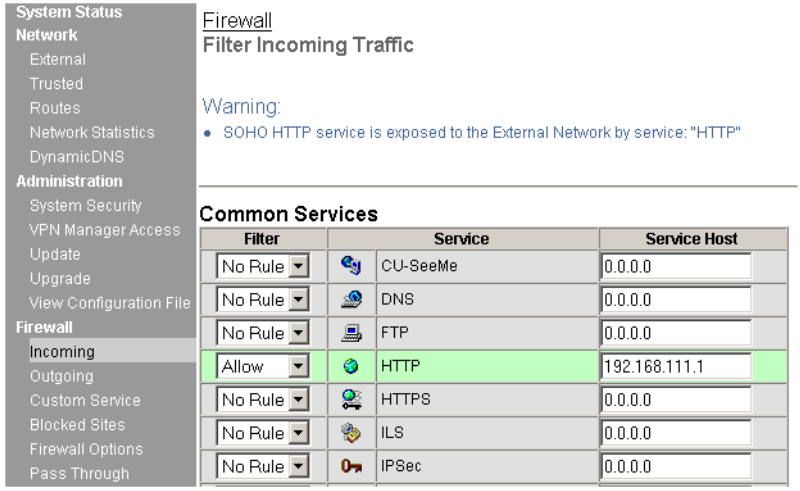
It is important to remember that each service you add opens a small window into your trusted network and marginally reduces your security. This is the inherent trade-off between access and security.

Pre-configured Services

Each service is defined by a combination of Internet protocols and port numbers to uniquely identify the connection type to applications and servers on the Internet. The SOHO 6 configuration pages include several of the most common types.

Follow these steps to add an Incoming service:

1 From the navigation bar on the left side, select **Firewall ⇒Incoming** or **Outgoing**.
The Filter Traffic page appears.



2 Locate a pre-configured service, such as FTP, Web, or Telnet, then select either **Allow** or **Deny** from the drop list.
In our example, the HTTP service is set to Allow enabling Web traffic incoming.

3 Enter the trusted network IP address of the computer to which this rule applies.
In our example, 192.168.111.2.

4 Click **Submit**.

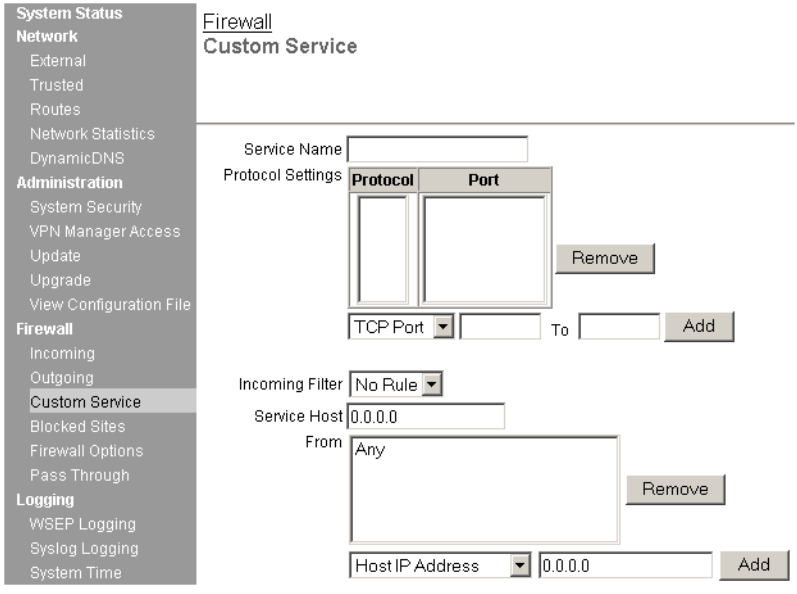
Create a Custom Service

In addition to the pre-configured services provided by the SOHO 6 configuration page, you can create custom services using either a TCP port, UDP port or specifying an IP protocol.

Follow these steps to create a custom service:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Firewall ⇒Custom Service**.
The Custom Service page appears.



3 Define a name for the service in the appropriate field.

4 Beneath the Protocol Settings fields, select either **TCP Port**, **UDP Port**, or **Protocol** from the drop list.
The Custom Service page refreshes.

NOTE

In addition to TCP and UDP ports, there are several other types of Internet protocols. To create a service for one of these protocols, you must define the protocol number—you cannot specify a port number.

5 Enter the port number (or numbers if creating a range of ports) or enter the IP protocol number to allow in the appropriate fields and click **Add**.

After creating a custom service, you need to specify a filter rule as well as define the incoming and outgoing properties.

6 At the Incoming and Outgoing Filter drop lists, select either **Allow** or **Deny**.

7 Select either Host IP Address, Network IP Address, or Host Range from the appropriate drop list.
The Custom Service page refreshes.

8 Enter either a single host IP address, a network IP address, or the start and end of a range of host IP addresses for this custom service in the appropriate fields.

9 Click **Add**.
Repeat the last three steps until all the appropriate address information for this custom service appears in the appropriate fields.

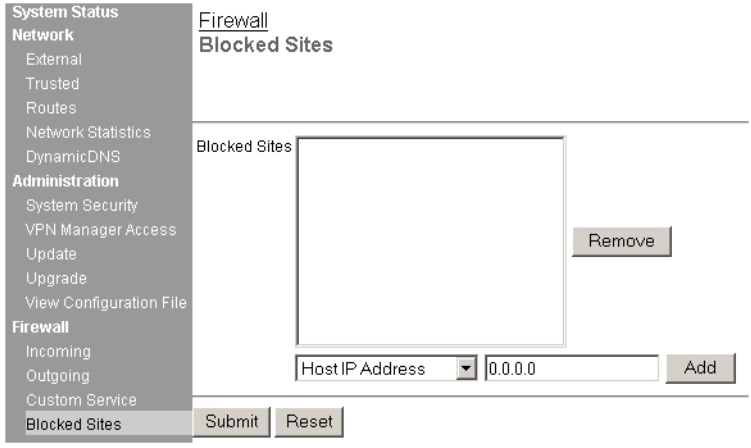
10 Click **Submit**.

Block External Sites

By default, the security stance of the SOHO 6 is to deny all incoming traffic to the trusted network, but to allow all outgoing traffic. However, you can selectively block access to particular Internet sites entirely.

Follow these steps to configure blocked sites:

1 From the navigation bar on the left side, select **Firewall ⇒Blocked Sites**.
The Blocked Sites page appears.



2 Select either Host IP Address, Network IP Address, or Host Range from the drop list.
The Blocked Sites page refreshes.

3 Enter either a single host IP address, a network IP address, or the start and end of a range of host IP addresses in the appropriate fields.
In our example, Host IP Address is selected and the IP address entered is 207.68.172.246.

4 Click **Add**.
The addressing appears in the Blocked Sites field.

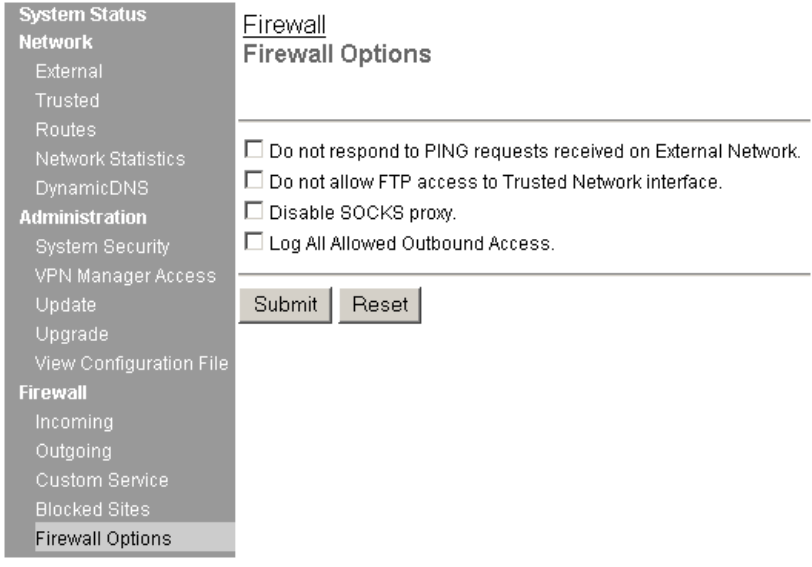
5 Click **Submit**.

Firewall Options

The SOHO 6 firewall feature includes a few rule settings that are less specific then the service settings discussed previously and are used to provide further security for your private network. These options are found on the Firewall Options page.

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Firewall ⇒Firewall Options**.
The Firewall Options page appears.



Ping requests received on the External Network

You can configure the SOHO 6 to deny all ping packets that it receives on the external interface.

1 Select **Do not respond to PING requests received on External Network**.

2 Click **Submit**.

Denying FTP access to the Trusted Network interface

You can configure the SOHO 6 to deny FTP access to the Trusted interface.

1 Select **Do not allow FTP access to Trusted Network**.

2 Click **Submit**.

SOCKS implementation for the SOHO 6

SOCKS is a network proxy filter that works with SOCKS-aware applications. A typical SOCKS-dependent application requires that several sockets be opened and made available to the Internet. When a SOCKS-aware application (ICQ is an example) registers with the SOCKS server, SOCKS is able to manage the need of the application to have many ports open.

To use an application with SOCKS, configure the application with the SOCKS server information.

Setting up your SOCKS application for use with the SOHO 6 requires no reconfiguration of the SOHO 6 appliance itself. Your SOHO 6 acts as the SOCKS proxy. You must, however, configure your application to be compliant with the SOHO 6 implementation of SOCKS version 5.

The SOHO 6 SOCKS feature has the following characteristics and limitations:

- SOHO 6 supports SOCKS version 5 only.
- It is a limited version of SOCKS and does not support authentication, nor does it support DNS (Domain Name System) resolution.

NOTE

Configure the particular application so that it does *not* attempt to make DNS look-ups with SOCKS. Some applications use only DNS through SOCKS and therefore do not function properly with the SOHO 6.

- Compatible SOCKS-aware applications that are used through the SOHO 6 include ICQ, IRC, and AOL Messenger.
- When you open a SOCKS application, it opens a "hole" in the SOHO 6 firewall making the computer running the application available to anyone on your trusted network. SOCKS applications therefore pose a significant security risk. To disable the port and close the security risk, see "Disabling SOCKS on the SOHO 6" on page 62.

Configuring your SOCKS application

Other than making certain that port 1080 is open to run a SOCKS-dependent application, the rest of the configuration tasks is done with the SOCKS-dependent application. Different applications may have variations in their settings, but you configure the SOCKS-dependent application, using the application user interface, to certain parameters allowing the SOHO 6 to pass SOCKS applications:

- If different services or versions of SOCKS are available, select SOCKS version 5.
- Select port 1080 for the application

- For the SOCKS proxy, enter the URL or IP address of the SOHO 6 trusted network. The default IP address is 192.168.111.1.

Disabling SOCKS on the SOHO 6

Once you use a SOCKS-compliant application through the SOHO 6, the primary SOCKS port is available to anyone on your trusted network. You can close this security gap between uses of SOCKS applications.

1 Enable the checkbox labeled **Disable SOCKS proxy**.
This disables the SOHO 6 from acting as a SOCKS proxy.

2 Click **Submit**.

When you need to use SOCKS again, follow this procedure:

1 Disable the checkbox labeled **Disable SOCKS proxy**.
This enables the SOHO 6 to act as a SOCKS proxy.

2 Click **Submit**.
The SOHO 6 is enabled again as a Proxy server and ready to pass SOCKS packets.

Logging all allowed outbound traffic

By default, the SOHO 6 logs only particular events and *not* all traffic passing through it. For the most part, the SOHO 6 records denied traffic. However, the SOHO 6 is able to record all allowed outbound traffic.

NOTE

This option will record an extensive amount of log entries. For this reason, WatchGuard recommends that you use it for diagnostic purposes only.

Follow these steps:

1 Select **Log All Allowed Outbound Access**.

2 Click **Submit**.

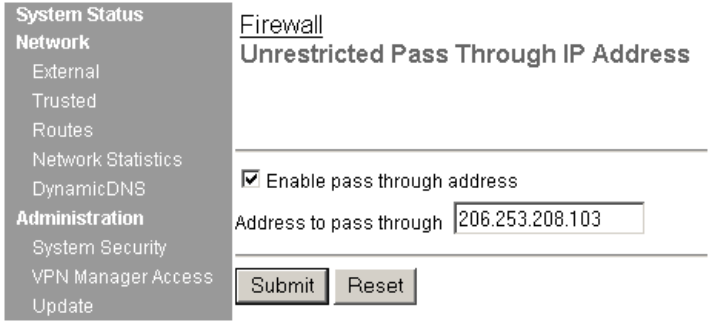
Create an Unrestricted Pass Through

The SOHO 6 is able to allow traffic to be passed through to a dedicated machine with a public IP address separated from the rest of the Trusted network.

Follow these steps to configure a pass through:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Firewall ⇒Pass Through**.
The Unrestricted Pass Through IP Address page appears.



3 Select **Enable pass through address**.

4 Enter the IP address to the pass through machine in the appropriate field. This *must* be a public IP address.
In our example, 208.253.208.103.

5 Click **Submit**.

NOTE

Use of the Pass Through feature increases the security risk to computers on the Trusted network. This is because the computer using the Pass Through resides on the same Ethernet segment as the Trusted network. If you are not completely and thoroughly familiar with the risks involved and Trusted network computers are not protected from potential threats, do not use the Pass Through feature

CHAPTER 7

Configure Logging

What is logging? Logging is the act of recording "events" that occur at the SOHO 6 interfaces. An event is any single activity, such as communication with the WatchGuard WebBlocker database or incoming traffic passing through the SOHO 6.

Logging is intended to record the kinds of activities that indicate security concerns—most importantly denied packets. Certain patterns of denied packets can indicate the type of attack that is being attempted. Remember that if power to the SOHO 6 is removed the messages are lost.

View SOHO 6 Log Messages

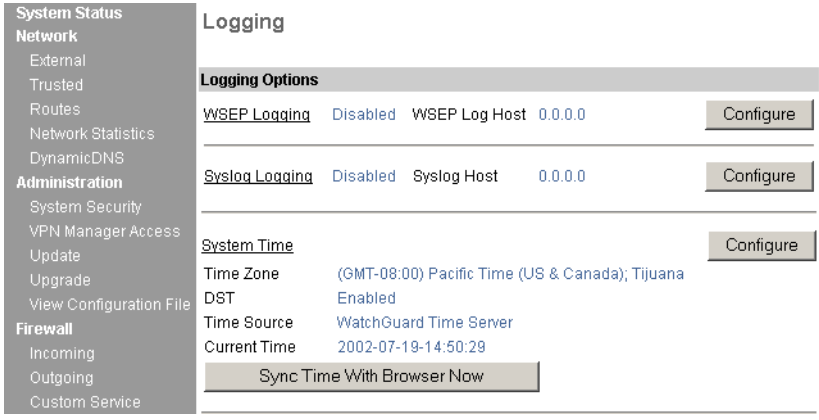
The WatchGuard SOHO 6 generates an ongoing activity log stored on the SOHO 6: the Event Log. This log stores a maximum of 150 messages. When it reaches this limit, the oldest message is deleted.

The log messages include time synchronizations between the SOHO 6 and the WatchGuard Time Server, discarded packets for a packet handling violation, duplicate messages, or return error messages and IPSec messages.

To view these messages:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1.

2 From the navigation bar on the left side, select **Logging**.
The Logging page appears and the Event Log is displayed in the lower portion of the page.



NOTE

The SOHO 6 displays the latest entry at the top of the Event Log.

To have your log messages synchronize with your computer:

- Click **Sync Time with Browser now**.

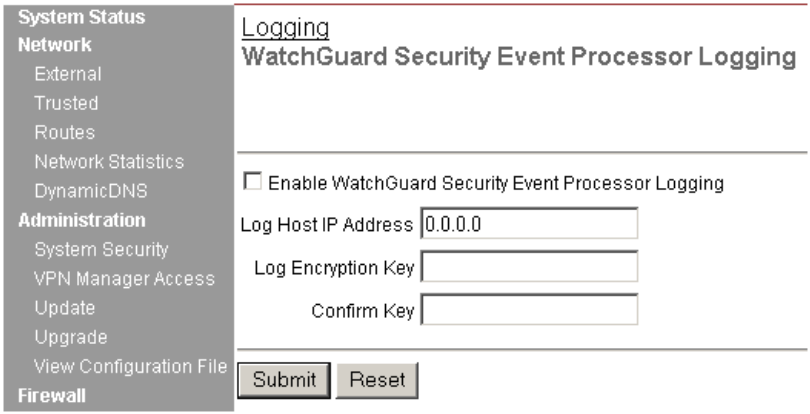
The SOHO 6 synchronizes the time at startup.

Set up Logging to a WatchGuard Security Event Processor Log Host

The WSEP (WatchGuard Security Event Processor) is an application available with the WatchGuard Firebox System software used by a Firebox II/III. The WSEP application runs on a dedicated log host and records log messages generated by the Firebox II/III. If you have a Firebox II/III and have configured the WSEP to accept logs from your SOHO 6, then follow these instructions to send your event logs to the WSEP.

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1.

2 From the navigation bar on the left side, select **Logging ⇒WSEP Logging**.
The WatchGuard Security Event Processor page appears.



3 Select **Enable WatchGuard Security Event Processor Logging**.

4 Enter the IP address of the WSEP server that is your log host in the appropriate field.
In our example, 192.168.111.5.

5 In the **Log Encryption Key** field, enter a passphrase and confirm it.

6 Click **Submit**.

NOTE

This encryption key must be identical to the one used in the WSEP.

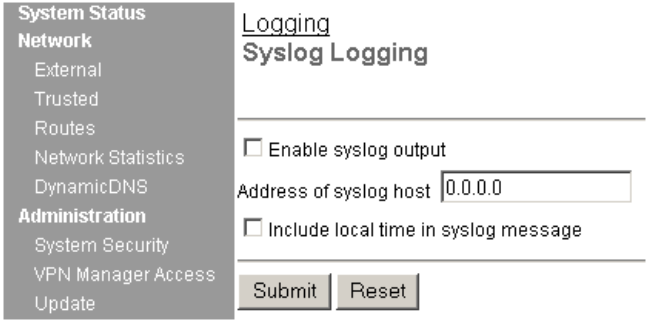
Set up Logging to a Syslog Host

The SOHO 6 also sends log entries to a Syslog host.

Follow these steps to setup a Syslog Host:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1.

2 From the navigation bar on the left side, select **Logging ⇒Syslog Logging**.
The Syslog Logging page appears.



3 Select **Enable syslog output**.

4 Enter the IP address of the Syslog server.
In our example, 206.253.208.100.

5 Click **Submit**.

To adjust your syslog messages to your browsers local time:

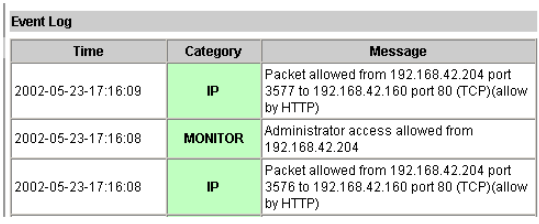
- Select **Include local time in syslog message**.

NOTE

Syslog traffic is not encrypted and use of this option creates a potential security risk when the information is sent over the Internet. However, if this traffic is sent through a VPN tunnel the traffic is encrypted with IPSec technology and therefore less of a security risk.

Set the System Time

The SOHO 6 stamps each log entry with the time that the event occurred.



Event Log

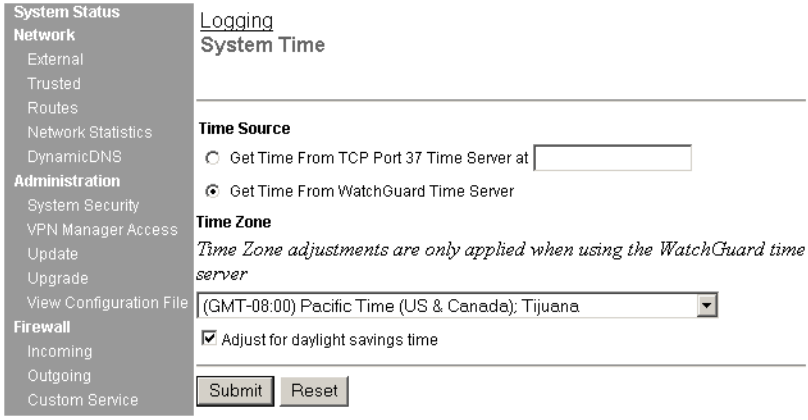
Time	Category	Message
2002-05-23-17:16:09	IP	Packet allowed from 192.168.42.204 port 3577 to 192.168.42.160 port 80 (TCP)(allow by HTTP)
2002-05-23-17:16:08	MONITOR	Administrator access allowed from 192.168.42.204
2002-05-23-17:16:08	IP	Packet allowed from 192.168.42.204 port 3576 to 192.168.42.160 port 80 (TCP)(allow by HTTP)

The log entry time stamp displays the time of day according to the settings for the system time.

To set the system time:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1.

2 From the navigation bar on the left side, select **Logging ⇒System Time**.
The System Time page appears.



If you have decided to use the WatchGuard Time Server:

3 Select **Get Time From WatchGuard Time Server**.

Or, to use a TCP Port 37 Time Server:

4 Select **Get Time From TCP Port 37 Time Server at**.

5 Enter the IP address of the time server in the appropriate field.

6 Click **Submit**.

To adjust your log messages for daylight savings time or set the time zone:

- Select **Adjust for daylight savings time**.
- Select a time zone from the drop list.

  Time Zone adjustments are only applied when using the WatchGuard time server.

CHAPTER 8

VPN—Virtual Private Networking

This chapter describes an optional feature of the WatchGuard SOHO 6, Virtual Private Networking (VPN) with IPSec.

Why Create a Virtual Private Network?

Virtual Private Networking (VPN) tunnels enable you to securely connect computers in two locations without requiring expensive, dedicated point-to-point data connections. With VPN, you use low cost connections to the Internet to create a virtual connection between two branch offices. Unlike a simple, unencrypted Internet connection, a VPN connection eliminates any significant risk of data being read or altered by outside users as it traverses the Internet.

What You Need

- One WatchGuard SOHO 6 with VPN and an IPSec-compliant appliance.

NOTE

While you can create a SOHO 6 to SOHO 6 VPN, you can also create a VPN with a WatchGuard Firebox II/III, Firebox Vclass, or other IPSec-compliant appliances.

- The following information from your Internet service provider for both appliances:
  - Static IP address
  - Primary DNS (Domain Name Service) IP address (optional)
  - If available, a secondary DNS address
  - Domain name (optional)
- Network addresses and subnet mask for networks. By default, the Trusted network address of the SOHO 6 is 192.168.111.0 and the subnet mask is 255.255.255.0.

NOTE

The internal networks on either end of the VPN tunnel must use different network addresses.

To create an IPSec tunnel between appliances you must add information to the configuration files of each that is specific to the site, such as external and trusted IP addresses. It is imperative to keep these addresses accurate. WatchGuard recommends making a table of IP addresses such as the one outlined below.

IP Address Table (example):

Item	Description	Assigned By
External IP Address	The IP address that identifies the SOHO 6 to the Internet. **Site A:** 207.168.55.2 **Site B:** 68.130.44.15	ISP
External Subnet Mask	The overlay of bits that determines which part of the IP address identifies your network. For example, a Class C address licenses 256 addresses and has a netmask of 255.255.255.0. **Site A:** 255.255.255.0 **Site B:** 255.255.255.0	ISP
Local Network Address	A private network address used by an organization's local network for identifying itself within the network. A local network address cannot be used as an external IP address. WatchGuard recommends using an address from one of the reserved ranges: 10.0.0.0/8 172.16.0.0/12—255.240.0.0 192.168.0.0/16—255.255.0.0 **Site A:** 192.168.111.0/24 **Site B:** 192.168.222.0/24	You
Shared Secret	A phrase stored at both ends of the tunnel to authenticate the transmission as being from the claimed origin. The secret can be any phrase, but mixing numerical, special, alphabetical, and uppercase characters improves security. For example, "Gu4c4mo!3" is better than "guacamole" **Site A:** OurLittleSecret **Site B:** OurLittleSecret	You
Encryption Method	Encryption method determines the length in bits of the key used to encrypt and decrypt communication packets. DES is a 56-bit encryption; 3DES is 168-bit, and much more secure. It is also slower. Select either 3DES or DES as long as both sides use the same method. **Site A:** 3DES **Site B:** 3DES	You

Authentication	Both sides must use the same method. **Site A:** MD5 (or SHA1) **Site B:** MD5 (or SHA1)	You

Enable the VPN Upgrade

You must first redeem the VPN upgrade license key before configuring VPN. Activating the VPN upgrade requires:

- An installed SOHO 6
- Internet connectivity
- A VPN upgrade license key

Step-by-step Instructions for Configuring a SOHO 6 VPN Tunnel

WatchGuard has developed a series of step-by-step instructions to facilitate configuration for a SOHO 6 VPN tunnel to any of several other IPSec-compliant appliances. To download these instructions using your Web browser, go to:

https://support.watchguard.com/support/interopvpn.asp

Special Considerations

Consider the following before configuring your WatchGuard SOHO 6 VPN network:

- You can connect only two appliances together: a WatchGuard SOHO 6 and either another SOHO 6 or another IPSec-compliant appliance. To set up multiple VPN tunnels, you need at least one WatchGuard Firebox II/III configured with the WatchGuard VPN Manager.
- Each appliance must be able to send messages to the other. If either appliance has a dynamically assigned IP address (see "Network addressing" on page 31 for an explanation of dynamic IP addresses), that appliance cannot find its remote counterpart.
- Both appliances must use the same encryption method. The two choices are DES or 3DES. When connecting two Microsoft Windows NT® networks, the two networks must be in the same Microsoft Windows domain or be trusted domains. This is a Microsoft Networking design implementation and not a limitation of the SOHO 6.

Frequently Asked Questions

Why do I need a static external address?

To create a VPN connection, one SOHO 6 must be able to find its partner appliance. If the addresses are allowed to change, the SOHO 6 will not find its remote computer.

How do I get a static external IP address?

Contact your ISP. Many systems use dynamically assigned addresses to simplify basic installations. Some providers also use this feature to discourage users from creating Web servers. These providers usually offer a static IP address option.

How do I connect three or four offices together?

To connect more than two offices together, WatchGuard recommends designating one office the center of a "star" network configuration and upgrading it to a WatchGuard Firebox. This makes it possible to manage multiple tunnels to SOHO 6s or other IPSec compliant appliances from the central Firebox.

How do I troubleshoot the connection?

If you are able to ping the remote SOHO 6 and computers behind it, your VPN tunnel is up and running. Any remaining problems are probably caused by the MS Networking or the applications being used.

Why is ping not working?

If you cannot ping the local network address of the remote SOHO 6, follow these steps to classify the problem:

1 Ping the external address of the remote SOHO 6.
For example, at Site A, ping 68.130.44.15 (Site B). You should get a reply. If not, verify the External network settings of Site B. If they are correct, verify that computers at Site B have access to the internet. If you are still having trouble, contact your ISP.

2 Once you are able to ping the external address of each SOHO 6, try pinging a local address.
From Site A, ping 192.168.111.1. If the tunnel is up, you should get a reply from the remote SOHO 6. If not, re-check the local settings page. Make sure that the local DHCP address ranges do not overlap. That is, IP addresses on either side of the tunnel *must not* be the same.

How do I obtain a VPN upgrade license key?

You can purchase them online. Using your Web browser, go to:

http://www.watchguard.com/sales/buyonline.asp

How do I enable a VPN Tunnel?

Full instructions for enabling a VPN tunnel are located at:

https://support.watchguard.com/AdvancedFaqs/sointerop_main.asp

MUVPN Clients

The SOHO 6 can be upgraded to use the MUVPN clients option. This feature allows single remote users to securely connect to the SOHO 6 through an IPSec VPN tunnel and access network resources on the Trusted network. Complete documentation on configuring your SOHO 6 once this upgrade option is purchased and redeemed are at:

https://www.watchguard.com/support/SOHOresources.asp

View the VPN Statistics

The SOHO 6 has a configuration page that displays a variety of VPN statistics to assist you in monitoring VPN traffic as well as troubleshooting potential problems.

To view the VPN Statistics page:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1.

2 From the navigation bar on the left side, select **VPN ⇒VPN Statistics**.
The VPN Statistics page appears.

CHAPTER 9

SOHO 6 WebBlocker

WebBlocker is an optional feature of the SOHO 6 that provides Web site filtering capabilities. It gives you precise control over the types of Web sites users on your trusted network are allowed to view.

How WebBlocker Works

WebBlocker relies on a URL database, the CyberNOT list, a service of CyberPatrol, owned and maintained by SurfControl. The WebBlocker database contains many thousands of IP addresses and directories. These addresses are divided into categories based upon content such as drug culture, intolerance, or sexual acts.

WatchGuard updates the Webblocker server with a new database at regular intervals.

Once you purchase and activate WebBlocker, every time a user on your trusted network attempts to reach an Internet Web site, the

SOHO 6 queries the WatchGuard database and determines whether or not to block the site. The SOHO 6 considers the following conditions in determining whether or not to block the site:

Web site not in the WebBlocker database

If the site is not in the WatchGuard WebBlocker database, the Web browser opens the page for viewing.

Web site in the WebBlocker database

If the site is in the WatchGuard WebBlocker database, the SOHO 6 checks whether or not to block that type (or category) of site. When the category is blocked, the browser displays a page informing the user that the site is unavailable for viewing. If the category is not blocked, the Web browser opens the page for viewing.

WatchGuard WebBlocker database unavailable

If for any reason the WatchGuard WebBlocker database is unavailable (for example, if there is briefly a problem between your ISP and the nearest WatchGuard server), the browser displays a page informing the user that the site is unavailable for viewing.

WebBlocker users and groups

Groups

A group is a collection of individuals or users of the system.

Users

These are individual members of a particular group.

Bypass the SOHO 6 WebBlocker

Occasionally, you may want to allow select individuals to bypass the filtering functions of SOHO 6 WebBlocker. For example, if you are using the SOHO 6 at a remote office as a telecommuter, you may want to block a particular category from your children while still retaining access to that information for the adults in the household.

The SOHO 6 WebBlocker configuration page includes a full access password field. Provide this password to those members of your trusted network allowed to bypass WebBlocker. When a site is blocked or unavailable, the user has the option of entering the full access password. With the password entered, the browser displays the otherwise blocked site. After the password is entered, the user is able to browse any site on the Internet until either the password expires or the browser is closed.

Purchase and Activate SOHO 6 WebBlocker

To use WatchGuard SOHO 6 WebBlocker, you must first purchase and enable the WebBlocker upgrade license key. For information on redeeming upgrade license keys, see, “Redeem your SOHO 6 Upgrade Options” on page 49.

Configure the SOHO 6 WebBlocker

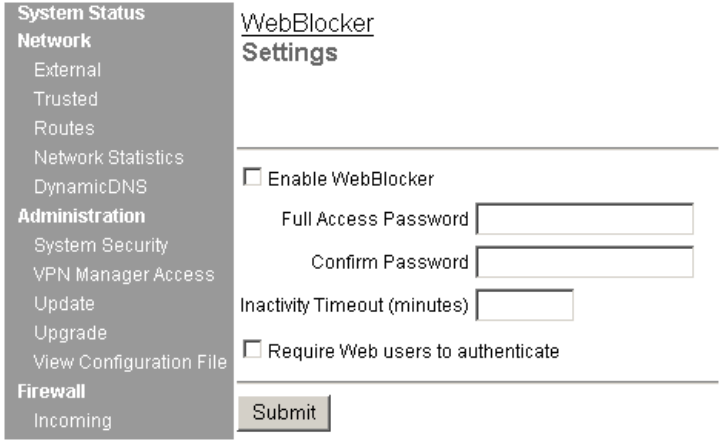
Use the WatchGuard SOHO 6 Configuration pages to activate WebBlocker, create a full access password for bypassing WebBlocker, define an inactivity timeout that sets the duration of the full access password, define the categories you want to block, and configure WebBlocker groups and users.

Activate WebBlocker

Follow these instructions to activate WebBlocker, create a full access password, define the inactivity timeout value, and require that your Web users authenticate (if your are using the groups and users feature option).

1 With your Web browser, go to the SOHO 6 Configuration Settings page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **WebBlocker ⇒ Settings**.
The WebBlocker Settings page appears.



3 Select **Enable WebBlocking**.

4 Enter the full access password.
The full access password allows a user a to bypasses otherwise blocked sites.

5 Enter the inactivity timeout in minutes.
For example, setting the inactivity timeout at 15 minutes ensures that unattended Web browsers are disconnected after sitting idle for 15 minutes.

6 If you intend to use WebBlocker groups and users, select **Require Web users to authenticate**.

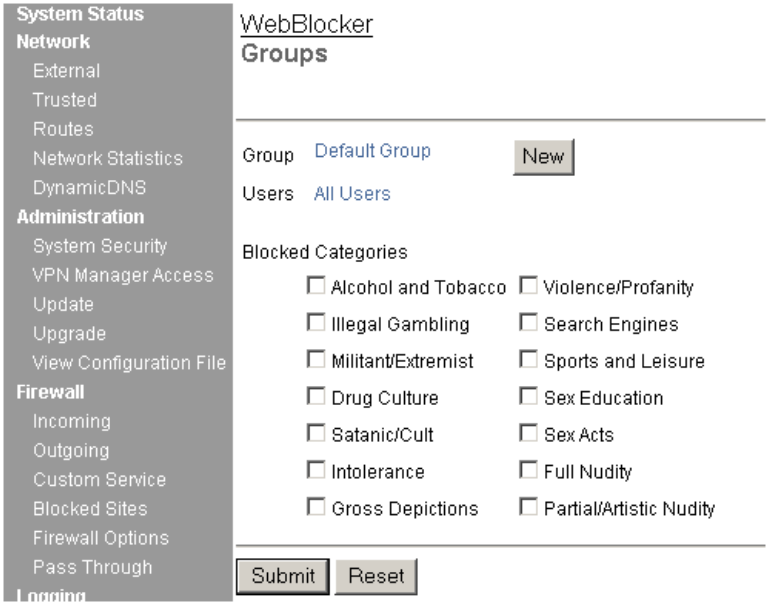
7 Click **Submit** to register your changes.

Create WebBlocker Groups and Users

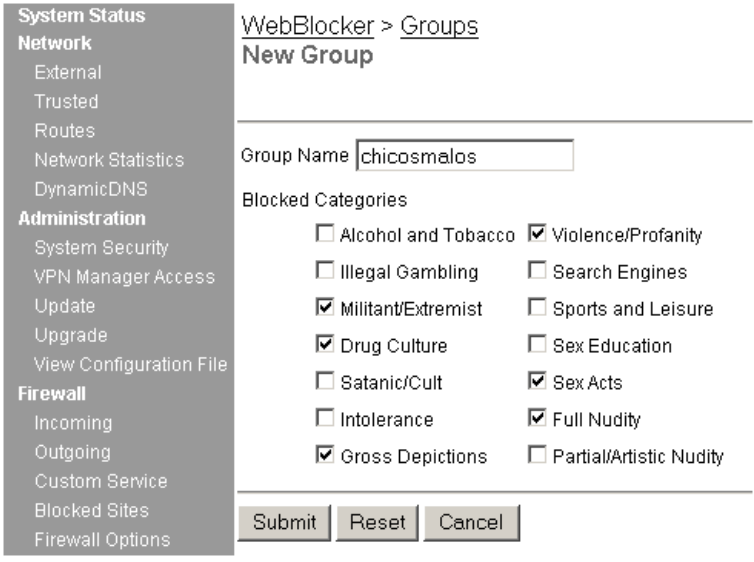
Follow these instructions to create WebBlocker Groups.

1 With your Web browser, go to the SOHO 6 Configuration Settings page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **WebBlocker ⇒Groups**.
The WebBlocker Groups page appears.



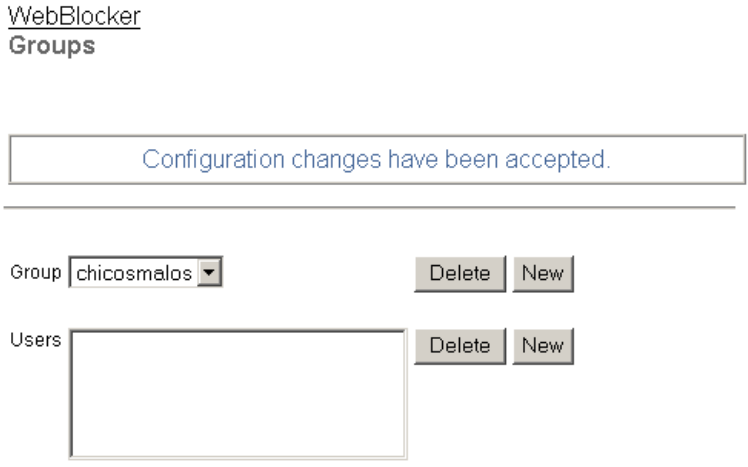
3 Click **New** to create a group name and profile.



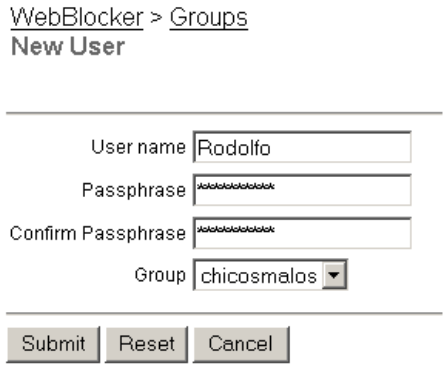
4 Define a Group Name and select the blocked categories for this group.

5 Click **Submit.**

A new Groups page appears indicating the configuration changes were accepted and are providing access.



6 To the right of the Users field, click **New**.
The New User page appears.



7 Enter a unique user name and passphrase (remember to confirm the passphrase). Use the Group drop list to assign the new user to a given group.

8 Click **Submit**.

NOTE

You can delete users or groups at any time by selecting them and clicking **Delete**.

WebBlocker Categories

WebBlocker relies on a URL database, the CyberNOT list, which is a service of CyberPatrol. The WebBlocker database contains thousands of IP addresses and directories. These addresses are divided into categories based on content such as drug culture, intolerance, or sexual acts. CyberPatrol constantly searches the Internet to update the list of blocked sites. The WebBlocker database contains the following 14 categories.

NOTE

All the categories of sites to be blocked are selected by advocacy rather than opinion or educational material. For example, the drugs/drug culture category blocks sites describing how to grow and use marijuana but does not block sites discussing the historical use of marijuana.

Alcohol/tobacco

Pictures or text advocating the sale, consumption, or production of alcoholic beverages and tobacco products.

Illegal Gambling

Pictures or text advocating materials or activities of a dubious nature that may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking

(using someone's phone lines without permission), and software piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, online sports, or financial betting, including non-monetary dares.

Militant/extremist

Pictures or text advocating extremely aggressive or combative behavior or advocacy of unlawful political measures. Topic includes groups that advocate violence as a means to achieve their goals. It also includes pages devoted to "how to" information on the making of weapons (for both lawful and unlawful reasons), ammunition, and pyrotechnics.

Drug Culture

Pictures or text advocating the illegal use of drugs for entertainment. This category includes substances that are used for other than their primary purpose to alter the individual's state of mind, such as glue sniffing. This does not include (that is, if selected these sites would not be WebBlocked under this category) currently illegal drugs legally prescribed for medicinal purposes (such as, drugs used to treat glaucoma or cancer).

Satanic/cult

Pictures or text advocating devil worship, an affinity for evil, wickedness, or the advocacy to join a cult. A cult is defined as: a closed society that is headed by a single individual where loyalty is demanded and leaving is punishable.

Intolerance

Pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability

or handicap, gender, or sexual orientation. Any picture or text that elevates one group over another. Also includes intolerant jokes or slurs.

Gross Depictions

Pictures or text describing anyone or anything that is either crudely vulgar, grossly deficient in civility or behavior, or shows scatological impropriety. Topic includes depictions of maiming, bloody figures, and indecent depiction of bodily functions.

Violence/profanity

Pictures or text exposing extreme cruelty or profanity. Cruelty is defined as: physical or emotional acts against any animal or person that are primarily intended to hurt or inflict pain. Topic includes obscene words, phrases, and profanity in either audio, text, or pictures.

Search Engines

Search engine sites such as AltaVista, InfoSeek, Yahoo!, and WebCrawler.

Sports and Leisure

Pictures or text describing sporting events, sports figures, or other entertainment activities.

Sex Education

Pictures or text advocating the proper use of contraceptives. Topic includes sites devoted to the explanation and description of condoms, oral contraceptives, intrauterine appliances, and other types of contraceptives. It also includes discussion sites devoted to conversations with partners about sexually transmitted diseases, pregnancy, and sexual boundaries. Not included in this category are commercial sites selling sexual paraphernalia (topics included under *Sexual Acts*).

Sexual Acts

Pictures or text exposing anyone or anything involved in explicit sexual acts and/or lewd and lascivious behavior. Topic includes masturbation, copulation, pedophilia, as well as intimacy involving nude or partially nude people in heterosexual, bisexual, lesbian, or homosexual encounters. It also includes phone sex advertisements, dating services, adult personals, and sites devoted to selling pornographic CD-ROMs and videos.

Full Nudity

Pictures exposing any or all portions of human genitalia. Topic does *not* include sites categorized as Partial/Artistic Nudity containing partial nudity of a wholesome nature. For example, it does not include Web sites for publications such as *National Geographic* or *Smithsonian* magazine nor sites hosted by museums such as the Guggenheim, the Louvre, or the Museum of Modern Art.

Partial/artistic Nudity

Pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia which is handled under the Full Nudity category. Topic does not include swimsuits, including thongs.

Search for Blocked Sites

To verify whether or not WebBlocker is blocking a site as part of a category block, visit the search/submit form on the Cyber Patrol Web site.

1 Using your Web browser, go to:

`http://www.cyberpatrol.com/cyberNOT/default.htm`

2 Scroll down to display the Cyber Patrol CyberNOT® Search Engine.

3 Type the URL of the site to check.

4 Click **Check if the URL is on the CyberNOT List**.

The search engine results notify you whether or not the site is on the CyberNOT list. Use this site also to suggest a new site for both the CyberNOT and CyberYES list, as well as to request a site review.

CHAPTER 10

Support Resources

Troubleshooting Tips

The following information is offered to help overcome any difficulties that might occur when installing and setting up your SOHO 6.

General

What do the PWR, Status, and Mode lights signify on the SOHO 6?

When the PWR light is lit, the SOHO 6 has power. When the Status light is lit, there is a management connection to the SOHO 6. When the MODE light is lit, the SOHO 6 is operational.

If the PWR light is *blinking*:

The SOHO 6 is running from its backup flash memory. You are able to connect to the SOHO 6 from a computer on one of the

four, numbered, Ethernet ports (labeled 0-3) and reload the configuration.

If the Mode light is *blinking*:

The SOHO 6 requires a DHCP assigned IP address for the external interface, but did not receive it. The WAN port is not connected to another appliance, the physical connection is faulty, or the other appliance is not operating properly.

How do I register my SOHO 6 with the LiveSecurity Service?

Register online by activating your bundled LiveSecurity® Service subscription. Activation entitles you to receive threat alert notifications, expert security advice, free anti-virus protection, software updates, technical support by web or phone, and access to extensive online help resources. To activate, make a note of your SOHO serial number, then use your Web browser to go to:

http://www.watchguard.com/activate.

For more information, see "Register your SOHO 6 and Activate the LiveSecurity Service" on page 27.

How do I restart my SOHO 6?

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 Click **Reboot**.

3 Wait for the SOHO 6 to complete the process. The MODE light on the front of the SOHO 6 will turn off, then back on. The SOHO 6 takes 30 seconds to boot up.

NOTE

You can also reboot by removing the power source for ten seconds, and then restoring power.

How do I reset my System Security password, if I forgot or lost it?

If you forgot your password, you must reset the SOHO 6 to its factory default. For instructions, see "Reset a SOHO 6 to factory default" on page 26.

How does the seat limitation on the SOHO 6 work?

The default user license on the SOHO 6 allows for ten users. The first ten computers on the network behind the SOHO 6 to access the Internet are allowed through the SOHO 6. To clear the list of these first ten computers you *must* reboot the SOHO 6.

What is a SOHO 6 Feature Key?

The Feature Key is an encrypted mask that tells the SOHO 6 which features are active. It is obtained by redeeming an upgrade option license key at the LiveSecurity Service Web site. You copy the Feature Key into a SOHO 6 configuration page and it is then stored in memory. For further instruction, see "Redeem your SOHO 6 Upgrade Options" on page 49.

I can't get a certain SOHO 6 feature to work with a DSL modem.

Some DSL routers implement NAT firewalls. Running NAT in front of the SOHO 6 causes problems with WebBlocker and the performance of IPSec. When a SOHO 6 is used in conjunction with

a DSL router, set the NAT feature of the DSL router to bridge-only mode.

How do I install and configure the SOHO 6 using a Macintosh (or other) operating system?

Installation instructions for the Macintosh and other operating systems are on the WatchGuard Web site at:

https://www.watchguard.com/pubs/install/index.asp

How do I know whether the cables are connected correctly to my SOHO 6?

There are fourteen lights on the front of the SOHO 6 grouped in pairs. The link light labeled WAN tells you if your SOHO 6 is connected to your modem. If this light is not lit, the SOHO 6 is not connected to your modem. Check to make sure that both sides of the cable are connected and that your Internet connection is active. The link lights labeled 0 through 3 correspond to the four numbered Ethernet ports of the trusted network. They tell you if the SOHO 6 is connected to a computer or hub. If the lights are not lit, the SOHO 6 is not connected to the computer or hub. Check to make sure that both sides of the cable are connected and that the computer or hub has power.

I can connect to the configuration screen; why can't I browse the Internet?

This means that the SOHO 6 is on, but something is wrong with the connection from the SOHO 6 to the Internet. Make sure the cable or DSL modem is connected correctly and has power. Also check the link light on your modem as well as the WAN link light on the SOHO 6.

If you continue to have trouble connecting to the Internet, call your ISP.

How can I see the MAC address of my SOHO 6?

A MAC (Media Access Control) address is a unique number used to identify the actual physical hardware of an Ethernet appliance.

1 With your Web browser, go to the SOHO 6 Configuration Settings page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 Towards the bottom of the System Status page, you see the External network header on the right side. Two MAC addresses are often listed.
Please note these addresses and have them ready if you need Technical Support.

Configuration

Where are the SOHO 6 settings stored?

The configuration parameters are stored in memory on the SOHO 6.

How do I set up DHCP on the trusted network of the SOHO 6?

1 Make sure your computer is set up to use DHCP. For instructions, see "Enable your computer for DHCP" on page 16.

2 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

3 From the navigation bar on the left side, select **Network ⇒Trusted**.

4 Select **Enable DHCP Server** and then click **Submit**.

How do I change to a static, trusted IP address?

Before you can use a static IP address, you must have a base Trusted IP address and subnet mask.

The following IP address ranges and subnet masks are set aside for private networks in compliance with RFC 1918. Replace the Xs in the network IP address with a number between 1 and 254. The subnet addresses do not need to be changed.

Network IP range	Subnet mask
10.x.x.x	255.0.0.0
172.16.x.x	255.240.0.0
192.168.x.x	255.255.0.0

To change to a static, trusted IP address:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Network ⇒Trusted**.

3 Disable **Enable DHCP Server** and then click **Submit**.

4 Enter the information. Click **Submit**.

How do I set up and disable Webblocker?

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **WebBlocker ⇒Settings**.
The WebBlocker Settings page appears.

3 Select **Enable WebBlocker**. Enter a full access password, and an inactivity timeout (in minutes).

To disable WebBlocker, deselect **Enable WebBlocker.**

How do I allow incoming services such as POP3, Telnet, and Web (HTTP)?

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Firewall ⇒Incoming**.
The Filter Incoming Traffic page appears.

3 Locate the pre-configured service you wish to allow in and select **Allow** from the drop list.

4 Enter the Trusted network IP address of the computer hosting the service.

5 Click **Submit**.

How do I allow incoming IP, or uncommon TCP and UDP protocols?

You need the IP address of the computer that is receiving the incoming data and the IP protocol number that corresponds to the specific incoming IP protocol. To allow an incoming IP protocol:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: http://192.168.111.1

2 From the navigation bar on the left side, select **Firewall ⇒Custom Service**.
The Custom Service page appears.

3 Beneath the Protocol Settings fields, select **TCP Port**, **UDP Port** or **Protocol** from the drop list.
The Custom Service page refreshes.

4 Enter a name for the service.

5 Enter the protocol number to allow in the Protocol field.

6 Click **Submit**.

7 From the navigation bar on the left side, select **Firewall ⇒Incoming**.
The Firewall Incoming Traffic page appears.

8 Near the bottom of the page, under the Custom Service header, locate the service you created and select **Allow** from the drop list.

9 Under the header Service Host, enter the IP address of the computer to which this traffic is allowed.

10 Click **Submit**.

VPN Management

Before setting up VPN, you must have:

- Two properly configured and working SOHO 6s or one SOHO 6 with the latest version of firmware and one Firebox II/III. Each SOHO 6 must have the VPN option activated.
- The static external IP address, the network address, and the subnet masks of both appliances. (The base trusted IP address of each SOHO 6 must be static and unique.)
- The DNS and WINS server IP address, if used.
- The shared key (passphrase) for the tunnel.
- The same encryption method for each end of the tunnel (DES or 3DES).
- The same authentication method for each end (MD-5 or SHA-1).

How do I set up my SOHO 6 for VPN Manager Access?

This requires the add-on product, WatchGuard VPN Manager software, which is purchased separately and used with the WatchGuard Firebox System software. To purchase VPN Manager, use your Web browser to go to:

https://www.watchguard.com/products/vpnmanager.asp

For more information on how to allow VPN Manager access to a SOHO 6, see the *VPN Guide*.

How do I set up VPN to a SOHO 6s?

For detailed information on how to configure a VPN tunnel between a SOHO 6 and another IPSec compliant appliance, use your Web browser to go to:

http://watchguard.com/support/sohovpn

1 Log in to the site.

2 Download the file you need.

3 Follow the instructions to configure your VPN tunnel.

Contact Technical support

(877) 232-3531	U.S.; End-user support
(206) 521-8375	U.S.; Authorized Reseller support
(360) 482-1083	International support

Online Documentation and In-Depth FAQs

WatchGuard maintains an extensive knowledge base consisting of product documentation in the form of printer friendly .pdf files, tutorials, In-Depth FAQs, and more. This information is available at:

https://support.watchguard.com/faqs/

Special Notices

- At the time of publication of this document, the online Help System has not been posted on the WatchGuard Web site. Therefore, clicking on the Help link at the top of the System Status page will redirect you to the WatchGuard Product Documentation page where you can find links to our knowledge base.

Index

100 indicator 7

A

Add Route page 38

B

blocked sites
  configuring 57
  in WebBlocker 92
  searching for 92
Blocked Sites page 57
browsers, supported 12
button, RESET 8

C

cables
  correct setup 98
  included in package 2
  required 12
configuration file, viewing 24, 51
custom incoming services, creating 55
Custom Service page 56, 101
Cyber Patrol 92

D

default factory settings 25–26
DHCP
  described 32
  setting up on Trusted Network 99
DNS service, dynamic 40
DSL modems, and SOHO 6 97
Dynamic DNS client page 40
dynamic DNS service,
  configuring 40–41
Dynamic Host Configuration Protocol.
  See DHCP
dynamic IP addresses
  configuring for 32
  described 31

E

events
  described 65
  logging, See logging
External Network
  denying ping packets received
    on 60

F

FAQs 104
feature keys 49, 97
filter rules, specifying for custom
  services 57
Filter Traffic page 54
Firewall Incoming Traffic page 102
Firewall Options page 59
firewall, specifying miscellaneous
  options 59
firmware
  updating 48
  viewing version of 24
FTP access, denying to the Trusted
  interface 60

G

Groups page 87

H

hardware description 6
HTTP proxy settings, disabling 14

I

incoming service, creating custom 55
indicators
  100 7
  link 7
  Mode 7
  WAN 7
installation
  cabling 19
  cabling for multiple computers 20
  determining TCP/IP settings 12
  disabling TCP/IP proxy settings 14
  items required for 12
Internet
  how information travels on 4
  problems browsing 98
IP addresses
  described 4
  disguising 5
  dynamic 31
  in networks 31
  maintaining table of 75

L

license keys, redeeming 49
licenses, upgrading 21
lights
  100 7
  link 7
  MODE 95
  Mode 7
  power 6
  PWR 95
  Status 7, 95, 96
  WAN 7
link indicator 7
LiveSecurity Service
  registering with 27
  renewing subscription 51
log host, setting WSEP 67
log messages
  contents of 66
  synchronizing with computer 67
  viewing 66
logging
  described 65
  to a WSEP host 67
  to Syslog host 69
Logging page 66

M

MAC address of SOHO 6 99
MacIntosh operating system 98
Mode indicator 7
MODE light 95
MUVPN clients option 79
MUVPN, license keys for 51

N

NAT 5
Network Address Translation (NAT) 5
Network Statistics page 39
network statistics, viewing 39
New User page 88
numbered ports 9

O

OPT port 8

P

pages
  Add Route 38

Blocked Sites 57
Custom Service 56, 101
Dynamic DNS client 40
Filter Traffic 54
Firewall Incoming Traffic 102
Firewall Options 59
Groups 87
Logging 66
Network Statistics 39
New User 88
Routes 38
SOHO 6 Administration 43
Syslog Logging 69
System Security 44, 45
System Status 23, 28
System Time 70
Unrestricted Pass Through IP Address 63
Update 48
Upgrade 50
View Configuration File 52
VPN Manager Access 47
VPN Statistics 80
WatchGuard Security Event Processor 67
WebBlocker Groups 85
WebBlocker Settings 84
Pass Through feature 64
passphrases
described 44
setting up 45
ping packets, denying all 60
Point-to-Point Protocol over Ethernet. See PPPoE
ports
numbered 9
numbers 5
OPT 8
WAN 9
power input 9
PPPoE
configuring for 34
described 32
pre-configured services, adding 54
protocols
allowing incoming 101
described 4
PWR light 6, 95

R

rebooting 28
rebooting on remote system 29
registration 27
Remote Management 46
RESET button 8
resetting to factory default 26
Routes page 38
routes, configuring static 38

S

seat licenses, upgrading 50
seat limitation 97
serial number, viewing 24
services
adding incoming 54
adding pre-configured 54
allowing incoming 101
and security risks 54
creating custom 55–57
creating custom incoming 55
described 5, 53
preconfigured 54
specifying filter rule for 57
sites
blocking 57
searching for blocked 92
SOCKS
configuring application 61
configuring for SOHO 6 60
described 60
disabling 62
SOHO 6 28, 29
and DSL modems 97
and MacIntosh operating system 98
and SOCKS 60
base model 27
configuring access to 43

configuring for dynamic addresses 32
configuring for PPPoE 34
configuring for static addressing 33
configuring VPN tunnel with 76
connecting to 23
default factory settings 25
described 2
firewall feature 59
front view 6
function of 3
hardware 6
installing 11–22
MAC address of 99
MUVPN clients option 79
package contents 2
ports 6, 8
rear view 8
registering 27
resetting to factory default 26
seat limitation 97
setting passphrase 45
setting up VPNs between 103
troubleshooting 95–103
upgrading 49
upgrading user license 21
viewing log messages for 66
SOHO 6 Administration page 43
SOHO Remote Management 46
static IP addresses
and VPNs 77
obtaining 78
static IP addressing, configuring for 33
static routes, configuring 38
Status light 7, 95, 96
Syslog Logging page 69
System Security page 44, 45
System Status page 23, 28
System Time page 70
system time, setting 70

T

TCP/IP settings, determining 12–14
technical support 104
time, setting 70
traffic
crearing unrestricted pass through 63
logging all outbound 62
traffic, monitoring 39
troubleshooting 95–103
Trusted Network
configuring additional computers on 36
denying FTP access to 60
Trusted Network Configuration page 37

U

Unrestricted Pass Through IP Address page 63
Update page 48
Update Wizard 49
upgrade license keys
redeeming 49
types of 50
Upgrade page 50
upgrading
seat licenses 50
user licenses 21
VPNs 51

V

View Configuration File page 52
VPN Manager
described 46
purchasing 103
setting up access to 46–47
setting up SOHO 6 for 103
VPN Manager Access page 47
VPN Statistics page 80
VPN upgrade
enabling 76
obtaining 79

VPNs
and SOHO 6, SOHO 6 tc 2
and static IP addresses 77
between two SOHO 6s 103
configuring with SOHO 6 76–79
connecting more than two offices 78
described 73
enabling tunnels 79
encryption for 77
license key for 51
requirements for 74, 102
special considerations for 77
troubleshooting connections 78
viewing statistics 79

W

WAN indicator 7
WAN port 9
WatchGuard Security Event Processor 67
WatchGuard Security Event Processor page 67
WebBlocker
activating 84
categories 89–92
configuring 84
creating users and groups for 85
database 81
described 81
enabling and disabling 100
purchasing and activating 83
searching for blocked sites 92
users and groups 83
WebBlocker Groups page 85
WebBlocker Settings page 84
WebBlocker upgrade, purchasing 83
WebBlocker, license key for 51
WSEP 67